GDPR Company Policy

Payment Assist

Table of Contents

1. Introduction

Payment Assist LTD is committed to conducting its business in accordance with all the applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Payment Assist LTD employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Payment Assist LTD customer (i.e. Data Subject).

Personal Data is any information (including opinions and intentions) which relate to an identified or identifiable natural person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about it is known as a Data Controller. Payment Assist LTD, as a data controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Payment Assist LTD to complaints, regulatory action, fines and/or reputational damage.

Payment Assist LTD's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all Payment Assist LTD employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanctions.

2. Scope

This Policy applies to all Payment Assist LTD entities where a Data Subject's Personal Data is processed:

- In the context of the business activities of the Payment Assist LTD entity.
- For the provision or offer of goods or service to individuals (including those provided or offered free-of-charge) by a Payment Assist LTD entity.
- To actively monitor the behaviour of individuals.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to the information about individuals.

This policy has been designed to establish a worldwide baseline standard for the processing and protection of Personal Data by all Payment Assist LTD entities. Where national law imposes a requirement, which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where nation law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to. If there are conflicting requirements in this policy and national law, please consult with the Data Protection Officer for guidance.

The protection of Personal Data belonging to Payment Assist LTD Employees is not within the scope of this policy. It is covered in the Payment Assist LTD 'Data Protection for Employee Data' policy.

3. Definitions

Employee	An individual who works in any capacity for Payment Assist LTD under a contract of employment, whether oral or written, expressed or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.
Third Party	An external organisation with which Payment Assist LTD conducts business and is also authorised to, under the direct authority of Payment Assist LTD, process the Personal Data of Payment Assist LTD customers and contacts.
Personal Data	Any information (including opinions and intentions) which relate to an identified or identifiable Natural Person.
Contact	Any past, present or prospective Payment Assist LTD customer.
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, on online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purpose and means of the Processing of Personal Data.
Data Subject	The identified or Identifiable Natural Person to which the data refers.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Definitions

Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulations set fourth in national law.
Data Processors	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller
Consent	Any freely given, specific, informed or ambiguous indication of the Data Subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.
Profiling	Any form pf automated processing of Personal Data where the Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement.
Binding Corporate Rules	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a jointly economic activity.

3. Definitions

Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Encryption	The process of converting information or data into code or redacting data to prevent unauthorised access.
Pseudonymisation	Data Amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a “key” that allows the data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

4. Policy

4.1.1 Governance

4.1.1 Data Protection Officer

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, Payment Assist LTD has established a dedication Data Protection Officer, with the following duties included and covered:

- Informing and advising Payment Assist LTD and its Employees who carry out Processing pursuant to Data Protection regulations, national law or Union based Data Protections provisions;
- Ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions;
- Providing guidance with regards to carrying out Data Protection impact assessments (DPIAs);
- Acting as a point of contact for the cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of Payment Assist LTD's current or intended Personal Data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of Payment Assist LTD's current or intended Personal Data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;
- Informing senior managers, officers and directors of Payment Assist LTD of any potential corporate, civil and criminal penalties which may be levied against Payment Assist Ltd and/or its Employees for violation of applicable Data Protection laws.

4. Policy

4.1.1 Data Protection Officer (Continued)

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with the Policy by any Third Party who;

- Provides Personal Data to a Payment Assist LTD entity
- Receives Personal Data from a Payment Assist LTD entity
- Has access to Personal Data collected or processed by a Payment Assist LTD entity.

4.1.2 Policy Dissemination & Enforcement

The management team of Payment Assist LTD must ensure that all Employees responsible for the Processing of Personal Data are aware of and comply with the contents of this policy.

In addition, Payment Assist LTD will make sure all Third Parties engaged to Process Personal Data on their behalf (i.e their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to gaining them access to the Personal Data controlled by Payment Assist LTD.

4. Policy

4.1.3 Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each must go through an approval process before continuing.

Payment assist LTD must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the senior management for review and approval. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of Personal Data.

4.1.4 Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by Payment Assist LTD in relation to this policy, will carry out annual checks to assess the following areas;

- The assignment of responsibilities.
- Raising awareness.
- Training of Employees.
- Data Subject rights.
- Personal Data transfers.
- Personal Data incident management and complaints handling.

The Data Protection Officer in cooperation with Payment Assist LTD key stakeholders will devise a plan, with schedule for correcting any identified deficiencies within a reasonable and defined timeline.

4. Policy

4.2 Data Protection Principles

Payment Assist LTD has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

- **Principle 1: Lawfulness, Fairness and Transparency.**

  Personal Data shall be protected lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, Payment Assist LTD must tell the Data Subject what Processing will occur (transparency). The Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulations (lawfulness).

- **Principle 2: Purpose Limitation**

  Personal Data shall be collected for specific, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means Payment Assist LTD must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

- **Principle 3: Data Minimisation**

  Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Payment Assist LTD must not store and Personal Data beyond what is strictly required.

- **Principle 4: Accuracy**

  Personal Data shall be accurate and kept up to date. This means Payment Assist LTD must have in place processed for identifying and addressing out-of-date, incorrect and redundant Personal Date.

4. Policy

4.2 Data Protection Principles (continued)

- **Principle 5: Storage Limitation**

  Personal Data shall be kept in a form which permits identification of Data Subjects for no longer that is necessary for the purposes for which the Personal Data is Processed. This means Payment Assist LTD must, wherever possible, store Personal Data in a way that limits or prevents identification of a Data Subject. This is to be no longer than 6 months after the final payment on any arrangement and cleared account.

- **Principle 6: Integrity & Confidentiality**

  Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Payment Assist LTD must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

- **Principle 7: Accountability**

  The Data Controller shall be responsible for and be able to demonstrate compliance. This means Payment Assist LTD must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

4. Policy

4.3 Data Collection

4.3.1 Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply;

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other that the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- A national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data.
- At the time of first communication if used for communication with Data Subject.
- At the time of disclosure of disclosed to another recipient.

4. Policy

4.3.2 Data Subject Consent

Payment Assist LTD will obtain Personal Data only by lawful and fair means, with full consent of the Data Subject using the below methods and techniques:

- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope and volition of the consents given.
- Providing a simple method for a Data Subject to withdraw their consent at any time.

4.3.3 Data Subject Notification

Payment Assist LTD will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data. When the Data Subject is asked to give consent to the Processing of the Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures. The Disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosure should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content and method of disclosure.

4.3.4 External Privacy Notices

Payment Assist LTD will include a ‘privacy and cookie notice’ on any website to fulfil the requirements by applicable law.

4. Policy

4.4 Data Use

4.4.1 Data Processing

Payment Assist LTD uses Personal Data of its contacts for the following purposes:

- The general running and business administration of Payment Assist LTD entities.
- To provide services to Payment Assist LTD customers.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by Payment Assist LTD to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Payment Assist LTD would then provide their details to the Third Parties for marketing purposes.

Payment Assist LTD will process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Payment Assist LTD will not process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given consent to the processing of their Personal Data.
- Processing is necessary for the performance of a contract to which the Data Subject is party to or to in order to take steps prior to Data Subject entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or Third Party (except where such interests are overridden by the rights and freedoms of the Data Subject).

4. Policy

4.4.1 Data Processing (Continued)

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Data Protection Officer before any such Processing may commence.

In any circumstance where consent has not been gained for the specific Processing in question, Payment Assist LTD will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for the intended further use.
- The context in which the Personal Data has been collected, regarding the relationship between Data Subject and Data Controller.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation and Pseudonymisation.

4. Policy

4.4.2 Special Categories of Data

Payment Assist LTD will only process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where on of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subjects.
- The Processing is necessary for the establishment, exercise or defence of legal claims.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another Natural Person where the Data Subject is physically or legally incapable of giving consent.

4.4.3 Data Quality

Payment Assist LTD will adopt all necessary measures to ensure that the Personal Data it collects, and Processes is complete and accurate in the first instance and is updated to reflect the current situation of the Data Subject. The measures adopted by Payment Assist LTD to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate or incomplete.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction rather than deletion of Personal Data, insofar as:
    - A law prohibits erasure.
    - Erasure would impair legitimate interests of the Data Subject.

4. Policy

4.4.4 Profiling & Automated Decision-Making

Payment Assist LTD will only engage in automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by law.

Where Payment Assist LTD utilises profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out.

Payment assist LTD must also ensure that all automated decision-making relating to a Data Subject is based on accurate data.

4.4.5 Digital Marketing

As a general rule Payment Assist LTD will not send promotional or direct marketing material to contacts through digital channels such as mobile phones, email and internet, without first obtaining their consent.

Where Personal Data Processing is approved for the digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object to having their data Processed.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of consent to carry out digital marketing to individuals providing they are given the opportunity to opt out.

4. Policy

4.5 Data Retention

To ensure fair Processing, Personal Data will not be retained by Payment Assist LTD for longer that necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

4.6 Data Protection

Payment Assist LTD will adopt physical, technical and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified or removed from a data processing system.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is Processed separately.
- Ensure that Personal Data is not kept longer than necessary.

4. Policy

4.7 Data Subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information Access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, Payment Assist LTD will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Data Protection Officer and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The recipients or categories of recipients to whom the Personal Data has been transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data and rationale for determining the storage period.
- The use of automate decision-making, including profiling.
- Lodge a complaint to the Data Protection Authority,
- Request rectification or erasure of their Personal Data where applicable.

4. Policy

4.7 Data Subject Requests (Continued)

All requests received for access to or rectification of Personal Data must be directed to the Data Protection Officer, who will log each request that is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Payment Assist LTD to correct or supplement erroneous, misleading, outdated or incomplete Personal Data.

If Payment Assist LTD cannot respond fully to the request within 30 days, the Data Protection Officer shall nevertheless provide the following information to the Data Subject, or their legal representative within the specified time:

- An acknowledgement of receipt of request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reasons for the refusal and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the Payment Assist LTD Employee who the Data Subject should contact to follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

4. Policy

4.8 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If Payment Assist LTD Processes Personal Data for one of theses purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If Payment Assist LTD receives a request from a court or any regulatory or law enforcement authority for information relation to a Payment Assist LTD contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

4. Policy

4.9 Data Protection Training

All Payment Assist LTD Employees that have access to Personal Data will have their responsibilities under the policy outlined to them as part of their staff induction training. In addition, Payment Assist LTD will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- The Data Protections Principles set forth in section 4.2 above.
- Each employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protection screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, print outs and electronic storage media.
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- Proper dispose of Personal Data by using secure shredding facilities.
- Any special risks associated with particular department activities or duties.

4. Policy

4.10 Data transfers

Payment Assist LTD may transfer Personal Data to internal or Third Party recipients located in another country where the country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e Third Countries), they must be made in compliance with an approved transfer mechanism.

Payment Assist LTD may only transfer Personal Data where one of the transfer scenarios list below applies:

- The Data Subject has given consent to the proposed transfer.
- The transfer is necessary for the performance of a conduct with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishments, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

4. Policy

4.10.1 transfer to Third Parties

Payment Assist LTD will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, Payment Assist LTD will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred will be set in place.

Where the Third Party is deemed to be a Data Processor and adequate Processing agreement with the Data Processor will be set in place. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process the Personal Data in compliance with Payment Assist LTD's instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

When Payment Assist LTD is outsourcing services to a Third Party (including cloud computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third County transfers of Personal Data. In either case, it will make sure to include, in cooperation with the Data Protection Officer, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

The Data Protection Officer shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the senior management team.

4. Policy

4.11 Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data Subject and the Data Protection Officer, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation or via complaint to the Data Protection Authority within the applicable jurisdiction.

4.12 Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Offices providing a description of what occurred. Notification of the incident can be made via email to compliance@payment-assist.co.uk or by calling 01664 503 151.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, they will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved.

All enquiries about this policy, including requests for exceptions or changes should be directed to the Data Protection Officer via email to compliance@payment-assist.co.uk

5. Policy Maintenance

5.1 Publication

This policy shall be available to all Payment Assist LTD entities and Employees through means deemed appropriate by the Data Protection Officer and senior management team.

5.2 Effective Date & Revisions

This policy is effective from the 11th of May 2018. Any revisions made to the policy will be made via the Data Protection Officer and they will solely be responsible for the maintenance and accuracy pf the policy. Notice of significant revisions shall be provided to all Payment assist LTD entities, Employees, Third Parties and all Data Controllers and Data Processors in relation to the requirement on the policy.

Changes made to this policy will come into force once published.

Appendix A – Information Notification to Data Subjects

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether consent has been obtained from the Data Subject.

Information Requiring Notification	With Consent	Without Consent
The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative	✔	✔
The Original source of the Personal Data, and if applicable, whether it came from a publicly accessible source		✔
The contact details of the Data Protection Officer, where applicable	✔	✔
The purpose and legal basis for Processing the Personal Data	✔	✔
The categories of Personal Data concerned	✔	✔
The recipients or categories of recipients of the Personal Data	✔	✔
Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further processing, with information on that purpose	✔	✔
Where the data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided	✔	✔
The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period	✔	✔
Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party	✔	✔
The existence of Data Subject rights allowing them to request from the Data Controller the information access, objection to processing, objection to automated decision-making, restriction of processing, data portability, data rectification and data erasure	✔	✔
Where Processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal	✔	
The right to lodge a complaint with a Data Protection Authority	✔	✔
The existence of automated decision-making (including profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such Processing for the Data Subject	✔	✔
Whether the provision of Personal Data is a statutory or contractual requirement, a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and if so the possible consequences of failure to provide such data	✔	✔

Appendix B – Adequacy for Personal Data Transfers

The following are a list of countries recognised as having an adequate level of legal protections for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.

- EU Countries (Austria, Belgium, Croatia, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)
- Iceland
- Liechtenstein
- Norway
- Andorra
- Argentina
- Canada
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- USA

The following are a list of Third Country transfer mechanisms that can provide adequate protection when transfers are made to countries lacking an adequate level of legal protections.

- Explicit Consent
- Binding Corporate Rules
- Codes of Conduct
- Certification Mechanisms
- DPA approved contracts between Data Controllers and Data Processors.