1. Introduction

1.1. When you visit the CardPay website of CardPay Ltd and CardPay Companies ("CardPay", "we" or "us"), correspond, apply or establish relations with us as a customer or partner, we process your data as a data controller.

1.2. This Privacy Notice sets out our current policies and commitment to data protection and privacy. In line with this, we aim to collect and process only data strictly necessary in the context of our relationship with (prospective) customers, (future) partners, users/visitors of our website(s) and online resources, in order to provide services and/or information for specific and legitimate purposes.

CardPay is dedicated to protecting the privacy and confidentiality of information in its possession, and is committed to appropriate use and protection of personal data, with transparency and respect for rights in accordance with EU Regulation 2016/679 (GDPR) and applicable data protection legislation ("data protection law").

We make our Privacy Notice available on our website www.cardpay.com in its most recent version. Please review it carefully. It contains information on how we collect, use, share and protect the personal data that we obtain.

2. Scope and General Provisions

2.1. This Notice should be read together and in conjunction with the relevant Terms and Conditions of the service/product (as applicable) provided by CardPay and applies also to use of our website and online systems pursuant to the relevant Terms.

2.2. This Privacy Notice applies to personal data held by CardPay as the data controller and as described in this Privacy Notice. It contains information on:

- The personal data we collect
- How we use personal data
- Who personal data might be shared with, and
- What rights are afforded

2.3. This Notice is addressed to natural persons ("data subjects") in the context of relationships that arise between CardPay and its Customers, where natural persons:

- Are Directors, signatories, representatives, shareholders, beneficial owners, secretaries, officers, employees of legal entities who are current or potential/applicant or former Customers
- Represent a legal entity/Customer, have applied to CardPay for a service/product offered by CardPay, are applicable users of a CardPay service/product, website or online system (e.g. internet-banking, payment card).

2.4. In this Notice, "Personal Data" (also, "personal information", "information", "data") refers to information that identifies you or may identify you (e.g. your name, address, identification number). "Processing" of Personal Data refers to actions such as collecting, handling, storing and protecting personal data.

2.5. Some links on CardPay websites may contain links or lead to non-CardPay websites or areas with their own data protection policies, which may differ from our Privacy Notice. Please ensure that the relevant policies of other entities are acceptable to you prior to using other sites or areas. Cardpay does not accept any responsibility or liability for third party websites. Additionally, if you are not a data subject to

whom this Notice is addressed, please refer to the privacy policy of the relevant data controller entity of your personal data to learn more about how the entity processes it.

3. Required Personal Data

3.1. The establishment and legality of contractual relations and provision of services between CardPay and its Customers is dependent on provision of the information requested by CardPay, which includes personal data of data subjects. It is an obligation to provide personal data to us:

- **Under our legal obligations** deriving from AML legislation and other legal acts. These require us to identify you, verify your identity and perform due diligence and enhanced due diligence if applicable on your person, as well as to fulfil our legal obligations under payment laws such as fraud prevention and other applicable laws.
- **For contractual purposes**. Establishment of business relations for provision of services, execution of transactions and for the performance of contractual obligations between both parties (CardPay and its Customers) requires provision of certain personal data.

3.2. Personal data is requested prior to the establishment and during the contractual relationship. Failure to provide requested data to us means that we will not be able to enter into a contract (establish business relations), or execute an order without requested data, or that we may no longer be able to continue with an existing relationship and provision of services and would have to terminate the relationship.

4. Collection and Use of Personal Data

Means of collection – How we collect data

4.1. We collect personal data from the following main sources:

- **Submitted data**
  This refers to data provided by you (or by the Customer on you) during account opening and in the course of the business relationship, via the application forms, via email or forms available on our website, or via other means of communication. In some cases, you may have previously provided your personal data to CardPay (e.g. in the context of an existing or former Customer relationship).
  By submitting personal data to CardPay, you are also acknowledging that CardPay may use this data in accordance with this Privacy Notice.

- **Data we collect when you use our services**
  This data may include:
  - Payment and transactions data
  - Profile and usage data (such as data when you connect to internet-banking, SMS services, and may include data on how you use the services. We may collect data from devices you use to connect to the services, such as computers and mobile phones, such as your IP address and using cookies (please refer to the Cookie Notice available on our website).

- **Third party data**
  Data we lawfully obtain from other entities such as service providers, information aggregation agencies, public authorities, persons that refer you to us, our Group companies, companies processing payments.

- **Public Data**
  Databases and publically accessible sources (e.g. Registrars of Companies, Commercial Registries, Media, the Internet)

4.2. Generally, submitted data constitutes the main source and means of collection of data; this data is provided by you/on you during the establishment of business relationship and during its course. Data is generated through the other sources is mainly based on/as a result of data from the main source.

Types of information - what we collect/process

4.3. Various types of personal data are collected and processed in the context of the relationship arising between you and CardPay and according to the service/product used and your capacity. Indicatively, the following are examples of categories and types of personal data may be processed:

Individual personal information	E.g. Name, previous names, data and place of birth, language, if you hold prominent public functions (PEPs), residence permit.
Individual personal contact details	E.g. Work address, home address, email address, telephone number, other contact details
Identity information	E.g. Passport, National ID card, Nationality, Utility bill, tax residence and tax ID
Financial information	E.g. Income, assets, financial status, source of wealth, personal bank details, professional status, employment field, employer details (including for example information such as certificates of directors/shareholders), level of education, property ownership, personal investments and income, loans, copy of payslips, tax returns, credit reference information.
Authentication data	E.g. Signature specimens, user logins.
Communications	E.g. Personal data that you may provide by filling in forms or by communicating with us (e.g. directed to us in letters, emails, via our electronic channels)
Transactional and other/documents information	E.g. Data arising for the execution of payment transactions (including data such as date, time, amount, currencies, beneficiary details, location information and details of merchant/ATM associated with the transaction), supplementary/supporting documentary evidence related to transactions, details arising from contractual obligations between CardPay and Customers.
Location and technical information	E.g. Location data (for example at the time of login or a transaction); technical information from/on devices and technology you use, IP addresses and device information, visitor's information and similar information collected automatically.
Publically available Data	E.g. Details about you from public records, media and information available on the internet
Documentary Data	E.g. Details about you stored in documents in different formats or copies of them.
Investigations data/results of due diligence and enhanced due diligence	E.g. Due diligence checks, sanctions and AML checks, Information to identify and manage fraud. We may also collect data regarding criminal convictions and offenses (special category of data), as part of its compliance measures with regulatory obligations, as well as other supporting documents and personal data related to the categories above.
Media	E.g. Closed circuit television (CCTV) at our offices (which may collect photos or videos of you).
Consents	E.g. Any permissions or consent given to us.

Purposes for which we use your personal data

4.4. You data is processed with the data minimization principle in mind. We aim to limit the processing of your data and the type of data processed to strictly the data needed for a lawful reason. The Company uses data inter alia to:

- Verify your identity (e.g. authentication, AML purposes and fraud prevention purposes)
- To provide the services requested (e.g. conduct Customer acceptance procedures to enter into business relations, opening of an account, issuing a payment instrument)
- To provide delivery channels (e.g. online systems)
- To execute transactions
- To execute requests, act upon instructions
- To perform our Contractual obligations
- To perform anti-money laundering checks and evaluations
- For crime prevention purposes and/or cooperation with authorities
- Use technology for decision making purposes
- Perform data analytics
- To maintain communication with you and provide you with up-to-date information
- To provide ongoing support, handle inquiries, complaints and similar issues
- To provide information in relation to the requested/provided products and services
- To provide information on products/services (this may be advertising/marketing)
- To enforce internal procedures and protective measures against fraud, risk and financial crime,
- For reporting purposes
- For internal operational support and administrative purposes (e.g. product development, audit, risk management).
- Obtain reports of an online problem (e.g. with the our website/online services)
- General administrative functions (e.g. maintenance of our internal records necessary for keeping up-to-date information in our systems, general record-keeping)
- Statistics and analytics for internal purposes and improvement of services and website
- Compliance with our legal obligations and regulatory framework
- Enforce or defend the rights of CardPay or CardPay Group members
- Ensure security and business continuity
- For service quality management and product improvement.

Legal bases - Lawful reasons for processing

4.5. When we process your personal data, we will rely on one of the processing legal bases below. We may process your personal data for more than one legal basis depending on the specific purpose for which we are using your data.

4.5.1. Performance of a contract

This is when processing of personal data is needed in order to perform our obligations under a contract (to provide services) concluded with Customers.
This is also processing in the course of the application to be able to complete our acceptance process of a potential Customer to be able to enter into a contract.

4.5.2. Legal obligation or for public interest

This is when we are required to process your personal data to comply with a legal obligation. CardPay is subject to various legal obligations, legal and regulatory requirements which include AML Laws and Laws on provision of e-money and payment services among others. We are also required to implement regulations and directives of several supervisory authorities including the Central Bank of Cyprus and European Banking Supervisors. The purposes of processing include verification controls of identity, money laundering and fraud prevention, compliance with our

record reporting obligations, tax obligations, risk control measures, as well as providing information to a competent authority, public body or law enforcement agency.

4.5.3. Legitimate interests

Where necessary, we may process personal data where there is a legitimate interest for us or a third party in pursuing commercial and business interests, except where such interests are overridden by your interests, fundamental rights and freedoms.

4.5.4. Your consent

In particular circumstances, we may ask you for specific permission to process personal information for specific purposes. Your data will be processed in this way if you agree to this. Where the legal basis is the consent you provided, you may withdraw your consent any time. The revocation of your consent will not affect the legality of the data processed prior to the revocation.

4.6. We have set out below for in a table format, an indicative description for your convenience, of the ways we may use your personal data as set out above, and which of the legal bases we may rely on to do so; we have also identified what our legitimate interests are and may be where appropriate.

Purpose (what we use your information for)	Lawful reason	Our Legitimate Interests
Acceptance processes to establish relationship: To review Customer's application	Performance of contract (to establish a contractual relationship) Legal Obligation Legitimate Interests	Compliance with applicable regulations governing the provision of Company's services Record Keeping Legal obligations during the review of an application
AML/TF, fraud prevention activities: To identify, examine, prosecute and prevent crime or fraud To verify Customer and identify his (continued) eligibility for the requested services and ability for management of the account To manage risk internally for the Company and externally for the Customers To comply with applicable laws and regulations To provide information to authorities upon request To respond and solve complaints	Legal Duty Public Interest Performance of contract Legitimate Interest	To establish and implement an internal fraud and crime identification and reporting mechanism Compliance with applicable regulations governing the provision of Company's services Cooperation with authorities at a national and international level To fulfill our legal and contractual obligations
Conducting of business relationship: To deliver the requested products and services To execute and manage customer's payment orders and to perform our obligations arising from Customer's transaction To apply on the Customer's account any fees and charges	Performance of contract Legal Obligation Legitimate Interest	Fulfilment of our legal and contractual duties Compliance with applicable regulations governing the provision of Company's services Company's interest in providing the requested services at a satisfactory and anticipated level

To collect any due funds To communicate with the Customer and provide information		Record Keeping maintenance
To provide information in relation to the (requested) products and services available To communicate with Customers and provide support to meet Customer's needs To manage relations of the Company with counterparties, partners, and service providers	Performance of contract Legal Obligation Legitimate interests	To ensure products and services are suitable for Customers To develop and improve products and services and to define applicable charges To identify the target market To fulfill our legal and contractual obligations
To improve services and products To manage our cooperation with other service providers To analyze Customers, and efficiency of operation of products and services To launch and test new products To develop new products and expand its business For Marketing activities	Performance of contract Legal Obligation Legitimate Interest	To develop and improve products and services and to define applicable charges To fulfill legal and contractual obligations
To manage the Company's operations, financial and business ability, communication channels and organizational planning	Legal Obligation Legitimate interests	Compliance with applicable regulations governing the provision of Company's services To fulfill its legal and contractual obligations
For proper execution and performance of the agreement between the Customer and the Company: To exercise rights set out in agreements To inform the Customer in relation to any changes to the Terms and Conditions of the services provided	Legal Obligation Performance of contract Legitimate interests	Compliance with applicable regulations governing the provision of Company's services To fulfill its legal and contractual obligations

5. Retention period

5.1. Our retention period is primarily determined by our obligations under applicable legislation to retain data for a specific period of time. Destruction will not be possible prior to the lapse of this period.
We are obliged to keep Customer data (including personal data) during the existence of the contractual relationship and for a minimum period of 5 years after its termination in accordance with AML legislation, unless legal or regulatory reasons prohibit us from destroying the data.

5.2. The retention period may be extended in case of other lawful reasons justifying longer retention (such as for complaints handling, legal proceedings, investigations, regulatory, tax, money laundering and crime and fraud prevention purposes).

5.3. For prospective Customers, personal data shall be kept for up to a year from the data of notification of the rejection of the application or from the data of withdrawal of the application, unless legal or regulatory reasons prohibit us from destroying the data or there is another lawful reason justifying longer retention (such as for complaints handling, legal proceedings, investigations, regulatory, tax, money laundering and crime and fraud prevention purposes).

6. Who receives your personal data

6.1. CardPay functions receive your personal data in the context of CardPay's operations. This is required in order to provide carry out requests and provide services, and to perform our contractual and legal obligations.

6.2. We will not share personal data with third parties unless this is necessary for our legitimate business needs, to carry out requests, provide services and/or as required or permitted by law. Third parties under these circumstances include:

6.2.1. Service providers
We will disclose personal data to third party partners and service providers (processors) so they can process it on our behalf where required. These service providers are required to provide sufficient assurances in accordance with data protection law. (e.g. being bound contractually to confidentiality and data protection obligations). We will only share personal data necessary for them to provide their services.

6.2.2. Auditors, advisors and consultants
We may disclose personal data for purposes and in the context of audits (e.g. external audits, security audits), to legal and other advisors, in order to investigate security issues, risks, complaints etc.

As such, personal data may be transferred and disclosed to:

- Money laundering and fraud prevention aggregation/agencies, compliance/verification services and risk prevention services. This is required in order to verify your identity, ensure protection against fraud, confirm eligibility for our services/products.
- Banks (other credit and financial service institutions), and similar institutions. These enable us to provide our services and include correspondent banks, intermediary banks.
- Payment Systems (SWIFT, SEPA, Visa, MasterCard, JCB, Unionpay), payment service providers, card processing companies. These enable us to provide our services.
- Card manufacturing/personalization and delivery companies. In order for us to create a personalized payment card and deliver it to the requested address
- Data management, storage, archiving, cloud storage service providers

- Companies assisting us with provision of our services (e.g. technological services, solutions, support such as support/maintenance/development of IT applications, technology, website management, telephony/SMS services)
- Customer support service providers and marketing service providers
- Entities of CardPay Group which are affiliated/related to us, acting as processors or controllers in order to provide services, streamlined services, ensure quality and effectiveness across the group
- Administrative service providers
- Auditing and accounting services and consultants
- External legal advisors

6.2.3. Regulatory authorities, law enforcement, courts

We may disclose personal data to comply with applicable legislation, regulatory obligations, to respond to requests of regulatory authorities, government and law enforcement agencies, courts and court orders in Cyprus/EEA/Internationally, such as:

- Supervisory Authorities including the Central Bank of Cyprus, European Central Bank, European Banking Authority
- FIU and the Police
- Tax Authorities
- Information Exchange Mechanisms
- Other regulators, authorities and public bodies wherever obligations exist

6.2.4. Other recipients may be any person/legal entity/organization for which you ask your data to be transferred to (e.g. reference etc.) or give your consent to transfer personal data.

6.2.5. We may also disclose your data in circumstances such as the following:

- If we are under a duty to disclose or share your personal data in order to comply with any legal or regulatory obligation or request,
- In order to apply or enforce the Terms and Conditions or any other agreement in place in the context of our relationship and to investigate potential breaches,
- In order to protect CardPay's rights, safety or property, or that of our customers or third parties/the public. This includes exchanging information with other companies and organizations for the purposes of money laundering, fraud prevention and equivalent risks,
- If CardPay or substantially all of its assets are acquired by a third party, in which case personal data held by it about its Customers will be one of the transferred assets.

Transfers outside the EEA or to international organisations

6.3. Your personal data may be transferred to third countries (outside the EEA) or to international organizations if the transfer is necessary and has a legal basis as described in this document. Such transfers take place for example:

- When necessary to carry out and in the context of transactions (e.g. card transactions, payment orders to third countries, through correspondent bank in third country)
- Under applicable law (e.g. tax legislation)
- On the basis of your instructions or consent
- In the context of data processing undertaken by third parties on our behalf. (e.g. the data may also be processed by staff operating outside of the EEA who work for CardPay or for one of our third party service providers or our Group. Such staff may be performing technical duties and support, duties related to processing of your orders, provision of support services etc.).

6.4. The processors (or controllers) in third countries in this case shall be either approved by the European Commission as providing adequate level of data protection or shall be have in place appropriate safeguards with the level of data protection in the EU. We aim to take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Notice (e.g. requirement to observe privacy standards equivalent to ours, maintaining security standards and procedures to prevent

unauthorised access, use of technology such as encryption and firewalls) to protect the security of data in transit and at rest.)

7. Automated decision-making and profiling

7.1. Automated decision-making means the process of making decisions through automated means of processing personal data, without human intervention. In establishing and carrying out a business relationship, we do not generally use automated decision-making.

7.2. We may process some specific data automatically, by using systems to make automated suggestions or decisions, including profiling, based on information we have or collect from other authorized sources. This helps us ensure we are able to react quickly and efficiently, with an aim also to protect our Customers. Automated decisions we may make include:
Detecting fraud : We are required to take anti-money laundering and anti-fraud measures. We may use your personal data to help us decide if an account/payment instrument is potentially being used for purposes of fraud or money-laundering/terrorist financing or sanctions contraventions. Such assessments are carried out in order to help us detect if an account/payment instrument is being used in ways fraudsters work or in a way unusual for you or the business of our Customer. If we determine there is a risk of fraud, unauthorized use, unusual activity, we may stop activity on the account/block the payment instrument and/or refuse access to them.

8. Website and Automatic collection - Cookies and IP addresses

8.1. CardPay's website contains forms with may be used by website visitors. When website visitors send us information online via forms on the website, in the context of provision of services, the information will be used for purposes and in ways set out in the Privacy Notice.

If you send us a CV/resume, we will use the information you provide to match you with available job positions, provided that a separate consent is given while the application for the position is completed prior to submission.

8.2. In some instances, CardPay and other entities (such as service providers) may use cookies and other technologies to collect certain types of data automatically when you visit CardPay websites and online platforms. The collection of this data enables CardPay to improve security, usability of CardPay's websites and online resources and to measure effectiveness of marketing activities. We may collect information about your computer or mobile device (including for example type of operating system and browser) for system administration.

For detailed information on cookies and the purposes for which we use them, please refer to our Cookie Notice available on our website.

8.3. An IP address is a number assigned to your computer when you access the internet, which allows computers and servers to recognize and communicate with one another. IP addresses of website visitors may be recorded for IT security and diagnostic purposes. This information may also be used in aggregate form to conduct website trend and performance analysis. In the context of provision of services, IP addresses may also be used for the purposes and in ways set out in with the Privacy Notice including fraud prevention.

9. Information on Data Security

9.1. CardPay has established security internal policies and procedures for secure processing of personal data in order to protect data from unauthorised access, loss, misuse, alteration or destruction. We ensure to the best of our abilities that access to personal data is limited to persons on a need to know basis, and that persons who have access are required to maintain its confidentiality. We utilise a series of technology and security solutions in order to protect data (such as storage of information you provide us on secure servers in the EEA, perimeter security mechanisms, such as encryption etc.). Nonetheless, security cannot be absolutely guaranteed against all threats despite our best efforts.

9.2. Transmission of information via the internet is not completely secure. We cannot guarantee the security of data transmitted to us via email, to our website or online resources; such transmissions are at your own risk.

9.3. Where you have access to our resources via user authentication means (e.g. user credentials), you are responsible for keeping your user credentials secure and confidential and not to disclose them to any persons. Please also consult our **security tips** available on our website.

10. Your Rights

Data Subject Rights

10.1. You have the following rights afforded under data protection law. These rights are afforded to natural persons who are data subjects of personal data which we hold as a controller. Please note that your rights are not absolute and may be limited due to a legal basis replied upon by us to process your data. As the majority of processing we perform is a consequence of legal obligations, some of the rights may be limited by our legal and regulatory requirements or legitimate interests.

10.1.1. Obtain a copy of your personal Data ("Right of access")

You can request a copy of the personal data retained and a confirmation from us whether personal data is processed or not.

10.1.2. Request correction of incorrect personal data

You can request a correction of incorrect or incomplete data kept by us. In such a case, we may need to verify the accuracy of the data we have and data provided and take steps to correct our records.

10.1.3. Object to the processing of personal data

You can object to the processing of personal data by us and request us to stop using the data in certain circumstances such as:

- Processing is conducted on the lawful ground of legitimate interest or of serving the public interest; however you object on grounds relating to your particular situation. In such a case, we may continue processing if we demonstrate that we have compelling legal grounds for processing which override your rights or that processing is necessary to establish, exercise of defend a legal claim.
  Please note that despite your objection, we may continue to use your personal data. This will be in cases where processing is required in compliance with legal obligations imposed on us (the requirements of legal obligations to process and retain data will supersede any right to objection.).
- Processing is conducted for marketing purposes.

In certain circumstances, if you objection to the processing of certain personal data, we may not be able to provide you services and may need to terminate provision of services.

10.1.4. Right to erasure ("to be forgotten")

You can request erasure of your personal data (depending on the circumstances and agreements in place) where:

- Processing is no longer required for the reasons the data was collected or processed
- We are relying on consent as a legal basis, and you withdraw your consent
- You have objected to the processing of data
- The data has been unlawfully processed (i.e. breach of legal basis requirement)

- Required by law

We may continue to retain you data if another legitimate reason for doing so exists. Our requirements to comply with legal obligations (record-keeping requirements in particular) to process and retain certain data will supersede any right to erasure requests, and we may also continue to retain/use your data if another legitimate reason for doing so exists (for exercise of legal claims and or serving in the public interest).

10.1.5. Restriction of processing of personal data

You can request that we restrict /suspend the use of personal data if:

- You requested that we verify the accuracy of your personal data we have
- Processing is unlawful but you do not request its erasure
- Processing and retention of data is no longer needed by us, but you wish that we retain it as this data is required by you to establish, exercise or defend a legal claim
- You have objected to the processing of data and are waiting for verification on our overriding legitimate interest

In some cases restriction might prevent the Company from performing its obligations under the contractual relationship with the Customer. In such event, we will notify Customer accordingly.

10.1.6. Withdrawal of consent

If we are relying on the lawful basis of your consent (i.e. we requested and you provided your consent), you can withdraw your consent at any time.

We may continue to process your information if another lawful basis exists for doing so. If we are unable to provide you with services due to the withdrawal of consent, we will inform you accordingly.

10.1.7. Data portability

You can request from us to provide personal data to you directly in an easily re-used format or to a third party if technically possible.
This right applies only to personal information provided by you to us for the performance of contractual relationship with us, or which we process based on your consent. This right may not be fully applicable in cases where the processing is done due to a legal obligation of the Company.

Exercising your rights

10.2. Please contact our DPO directly at contact details indicted below to exercise your rights or if you have questions about the use of your personal data.

10.3. You may be subject to identification procedures and measures in order to ensure that no personal data is disclosed to unauthorized persons. We may also request additional information/clarifications to process your request as rapidly and efficiently as possible.

10.4. All requests must be made in English in a comprehensive manner, and contain a clear description of the object of the request. We will not be able to process requests which are incomprehensive or in languages other than English.

10.5. We will not normally charge a fee to access your personal data (or exercise other rights). We may charge a fee where your request is clearly unfounded, excessive or repetitive. Alternatively, we may reject such a request as manifestly or excessively burdensome, unfounded and not submitted in good faith.

10.6. Depending on the complexity of your request and volume of data associated with it, we will aim to satisfy all legitimate requests within one month of receipt or to inform you of refusal, or of an extension period of up to three months to satisfy your request. We will notify you appropriately if your request requires more than one month to fulfill.

Right to file a complaint

10.7. If you have any complaints about the use of your data, exercise of your rights, please notify and/or file a complaint with our DPO directly at the contact details indicated below or fill out and submit the relevant form available on the Company's website: www.cardpay.com. We will immediately investigate and inform you in regards to your complaint.

10.8. Complaints must be made in English in a comprehensive manner, and contain sufficient details and a clear description of the complaint. We will not be able to process requests which are incomprehensive or in languages other than English.

10.9. You may also submit a complaint to the Commissioner for Personal Data protection. Information on filing is available on the Commissioner's website.

11. Data Protection Officer Contact details

CardPay has appointed a Data Protection Officer at its headquarters, who can address questions and concerns and can be contacted as follows:

Data Protection Officer
CardPay
125 Georgiou Griva Digeni, Limassol, 3101, Cyprus
Email: dpo@cy.cardpay.com

12. Your Responsibilities

12.1. You are responsible for ensuring that the information provided to CardPay by you/about you or on your behalf is accurate and up to date, and you must inform us if anything changes as soon as possible.

12.2. If you provide information about another person, you must direct them to this Privacy Notice and ensure they also agree to CardPay using their information as described in it.

13. Changes to our Privacy Notice

13.1. We may revise or update this privacy notice from time to time. In such a case, we make the most recent version of the Privacy Notice available on our website www.cardpay.com, informing you accordingly by displaying in the updated version and relevant date of update.

13.2. You are advised to visit our website frequently to consult our Privacy Notice in its most recent version.