Privacy policy

Effective as of 25.05.2017

Last updated: 22nd of August 2019

This Privacy Policy describes how we collect, use, process, and disclose your information, including personal information, in conjunction with your access to and use of myPOS Service.

If you see an undefined term in this Privacy Policy (such as “myPOS Account” or “myPOS Card”), it has the same definition as in our Legal Agreement for myPOS Account, Legal Agreement for myPOS Card, Merchant Agreement or other legal documents regulating myPOS Service to all of which this Privacy Policy is inseparable part.

When this policy mentions “we,” “us,” or “our,” it refers to the respective company, providing myPOS Services to the Client, under the above-mentioned Legal Agreements, that is responsible for your information under this Privacy Policy (the “**Data Controller**”).

For the purposes of this documents myPOS Services consist of products, services, content, features, technologies, or functions, and all related websites, applications and services offered to you by us or mobile apps, online platform, official social media platforms, or other online properties through which we provide payment and e-money services.

We give utmost importance to the protection of personal data of our customers. In the following Privacy Policy, we inform the Client about the collection, use and processing of your personal data when you apply, register or use our myPOS Service and all functionalities, included in the Service, including our website https://www.mypos.eu (hereinafter: "Website"), our myPOS Mobile App, E-money account and Cards.

- For the purposes of providing myPOS Account under the Legal Agreement for myPOS Account with myPOS Europe Ltd. the responsible Data Controller is myPOS Europe Ltd, Company number 10630670, Registered office address at the Shard, Level 24, 32 London Bridge Street, London, SE1 9SG. (referred to as myPOS Europe Ltd., UK):
- For the purposes of providing myPOS Account under the Legal Agreement for myPOS Account with iCard AD the responsible Data Controller is iCard AD, Company number 175325806, Registered office Bulgaria, Varna, Business Park Varna, Building B1, PO 9009 (referred to as iCard AD, Bulgaria) and the main data processor is myPOS AD Company Number 205050564, with seat and registered address at Business Park Varna B1, Bulgaria, acting as an agent of iCard (referred to as “myPOS AD”);
- For the purpose of providing myPOS Card under the Legal Agreement for myPOS Card the responsible Data Controller is iCard AD, Bulgaria and the main data processor is myPOS AD;
- For the purposes of providing acquiring services under the Merchant Agreement the responsible Data Controller is iCard AD, Bulgaria;

This Privacy Policy also applies to the information that is collected and used in relation to myPOS Online Store pursuant to Conditions of Use myPOS Online Store.

- When you use the myPOS Online Store for the purposes of online ordering and purchasing myPOS Terminals, you will be also providing your personal information, to myPOS Services OOD, Bulgaria, Company number 204713889, with Registered office Business Park Varna No B1, Varna, Bulgaria which will also be the Data Controller of your information related to the myPOS Store;

Where one of the above mentioned entities is specified as responsible Data Controller we inform you that the other entities specified above are acting as Data Processors of the Date Controller and vice-versa. The ultimate liability lies with the respective Data Controller and you should address all your questions to the respective Data Controller via the contact details specified below.

For the purposes of providing Account, Acquiring and Card-related services, myPOS AD, Company Number 205050564, with seat and registered address at Business Park Varna B1, Bulgaria, acting as an agent of iCard, shall be the main Data processor in relation to your personal data.

myPOS Service is designed for business purposes and may be used by individuals or entities. In case you are registering for and/or using myPOS Services on behalf of an entity we will treat you as authorized person and you may be obliged to disclose to us personal data of the legal representatives, the employees, the agents, the beneficial owners or any other third-party related to the entity pursuant to the rules described below. You certify that where you have provided information regarding any third person beside yourself you have received prior consent from that other person to provide their personal information to us.

Not a Framework Contract: For the avoidance of doubt, this Privacy Policy does not constitute a "framework contract" for the purpose of the EU Payment Services Directive 2 (EU) 2015/2366 or any implementation of that directive in the European Union or EEA (including, without limitation any national laws implementing the EU PSD).

DISCLAIMER:

IN CASE MYPOS EUROPE LTD. DOES NO LONGER HAVE THE RIGHT TO PROVIDE CROSS-BORDER SERVICES IN THE EUROPEAN UNION FOR LEGAL REASONS, THE FORMER SHALL CONTINUE TO PROCESS DATA OF ITS EUROPEAN UNION CLIENTS ONLY FOR THE PURPOSES OF COMPLYING WITH REGULATORY RETENTION PERIODS.

ALL CLIENTS, FOR WHICH MYPOS EUROPE LTD. HAS ACTED AS A DATA CONTROLLER, IN THE ABSENCE OF THEIR EXPLICIT REFUSAL, SHALL THENCEFORTH BE SERVICED BY ANOTHER E-MONEY INSTITUTION AND THEREFORE THAT E-MONEY INSTITUTION SHALL BECOME THE RESPONSIBLE DATA CONTROLLER FOR SAID CLIENTS' DATA.

1. WHAT INFORMATION WE COLLECT

You are informed that there are three general categories of information that is collected from you differentiated on grounds as defined by the Regulation 2016/679 and other applicable data protection national laws.

1.1 Information That We Collect In Order To Perform Our Legal Obligations and In Order To Provide myPOS Service As Part Of Our Contract With You

We ask for and collect from you the following personal information when you use the myPOS Service.

This information is necessary for us to comply with our regulatory obligations and for the adequate performance of the contract between you and us. Without it, we may not be able to provide you effectively with myPOS Service for which you register.

- **Registration and Use of Account Information**. When you sign up for myPOS Service, we require certain personal information such as:
    - First name and surname;
    - Date of birth;
    - Place of birth;
    - Email address;
    - Nationality;
    - Registered address;
    - Mobile telephone number;
    - Identification document and all data from the identification document;
    - Type of identification document;
    - Issue date;
    - ID number;
    - Issuing authority;

And other data which we may choose to collect in our enrol forms, which is necessary for your identification and verification.

- **Identity Verification Information**. In accordance with our legal obligations under the relevant Anti-money laundering and anti-terrorism financing regulations, we are obliged to verify your identity or the identity of the authorized user who is opening the Account (in case of company or other entity, referred to as "user opening the Account").

We comply with this legal obligation by means of online-based Video Identification Chat ("video call") and other procedures for verification in compliance with applicable AML laws. The Video Call is conducted by the employees of licensed as E-money institution, iCard AD, Bulgaria, Varna, Business Park Varna, Building B1, PO 9009, or by employees of iCall EOOD, Company number 204259408, with Registered office Business Park Varna No B1, Varna, Bulgaria, which act as a sub-contractor to us for the purposes of customer support and to which you agree to provide your personal data. We shall provide a secure video channel and the necessary level of direct visual communication connection with the mobile device of the Client or user opening the Account via Mobile App. To achieve the effective execution of the Video Identification Call you or the user opening the Account must give us access to the camera of the mobile device. During the video call, in order to fully comply with the relevant Anti-money laundering and anti-terrorism financing regulations, we must take:

- photographs of the user registering for myPOS Service; and

- photographs of the principal page of your or the user opening the account's passport or of the front and rear sides of any other official ID document.

For the same purposes you or user opening the Account you might have to allow us to download and read the chip embedder in the Passport/digital copy of the Passport (referred to as ePassport) if applicable. The personal data stored in the ePassport or other official ID document will be read and encrypted via NFC technology.

- **Tax information**. In order to comply with FATCA regulations, we are required to collect your Tax Identification Number ("TIN"), Country of Tax Residence and status (active or passive business). We might be required to disclose this information to its supervising tax authorities.
- **Risk and Fraud related information**. In order to comply with relevant Anti-money laundering and anti-terrorism financing regulations we collect personal data regarding you, such as demographic data or fraud detection information, from third party service providers and/or partners, and combine it with information we have about you.

For example, we may receive background check results (with your consent where required) or fraud warnings from service providers like identity verification services for our fraud prevention and risk assessment efforts. We may receive information about you and your activities on and off myPOS Service through partnerships, or about your experiences and interactions from our partner and networks.

- **Source of income, annual estimate over the account, business activity details**. In order to comply with relevant Anti-money laundering and anti-terrorism financing regulations we collect personal data regarding you related to your sources of income and any other similar financial information about you which would help us prevent money laundering and/or terrorism financing.
- **Payment Card-related information**. We collect information about your payment cards, which we have issued to you or which are issued to you by third-party issuers and are linked to your account. The information may be as follows: address of delivery of card, masked (first and last 4 digits) card number (PAN), issue date, expiry date, IBAN or other payment account identifier to which card is linked to, currency, card transaction data, spending limits, expired cards' details, SMS or other communication which the cardholder has received or has initiated with us, card status history, date of activation, linked cards or duplicates.
- **Log data and device information**. We automatically collect log data and device information when you access and use the myPOS Service, even if you have not created an myPOS Account or logged in. That information includes, among other things: details about how you've used the myPOS Platform (including if you clicked on links to third party applications), IP address, access dates and times, hardware and software information, device information, device event information, unique identifiers, crash data, cookie data, and the pages you've viewed or engaged with before or after using the myPOS Platform. We collect this information in relation to our legal obligation to provide you or our other clients with secure methods of controlling the financial assets and personal data.
- **Location**. We collect information for your location at the moment of registration, and, in certain cases, when you log in or out of the myPOS Platform. We process this information as part of our legal obligations related to AML/CTF due diligence checks. The myPOS Platform requires will ask you to turn on location sharing by enabling the "Location Information" on your device prior to finishing the registration procedure.
- **Payment Transaction Information**. We collect information related to your payment transactions under myPOS Service for example when you make purchases from merchants, you receive money transfers, you accept card payments, we process payments executed by you, or you send money to friends and family.

The payment transaction information may include the payment instrument's details used, date and time of transactions performed by you, amount of payment transaction, payment instrument expiration date and billing postcode, email address, IBAN or other account identifier information, your address and other related transaction details.

This information is necessary for the adequate performance of the contract between you and us and to allow us to provide you effectively the e-money and payment services.

- **Participant information** – When you use our myPOS Service, we collect Personal Data you provide us about the other participants associated with the transaction. Particular payment transaction information may include:
- **Send or request money**: When you send or request money through our service, we collect Personal Data such as name, postal address, e-mail, telephone number, and financial account information about the person who is receiving money from you or sending money to you. The extent of Personal Data required about a participant may vary depending on the Services you are using to send or request money.
- **Accept Card Payments**: When you accept card payments on your myPOS Terminal we collect payment details of the person performing the payment such as card number (PAN), issue date, expiry date, IBAN or other payment account identifier to which card is linked to, currency, amount of card transaction and other card transaction data.
- **Add value to your accounts**: If you use myPOS functionalities to add value to your Account or any other account you may have, or if you ask a third party to add value to any of these accounts, we may collect personal data from you about the other party, or from the other party about you to facilitate the request. For example, if you use our myPOS to reload a mobile phone, or to request value be added to your mobile account, we may collect Personal Data and other

information including mobile account number from the other participant.
- **Money transfers to or from other Financial institutions**: If you use myPOS functionalities to transfer money to accounts held with other Financial institutions we may collect personal data from you about the other party, or from the other party about you to facilitate the payment transaction, or provide the other Financial institutions with your Identity verification information. This is our obligation under Regulation 2015/847.

1.2 Information That We Collect With Your Consent

You may choose to provide us with additional personal information in order to obtain a better user experience when using myPOS. This additional information will be processed based on your consent.

- **Address Book Contact Information**. You may choose to give us access to your address book contacts or enter your contacts' information manually to access certain features of the myPOS, like sending payment requests or payment links with myPOS Service.
- **Additional Information**. You may otherwise choose to provide us information when you fill in a form, conduct a search, update or add information to your myPOS Account, respond to surveys, participate in promotions, or use other features of the myPOS Service.

1.3 Information We Collect from Your Use of the myPOS Service.

When you use the myPOS Service, we may collect information, including personal information, about the services you use and how you use them. This information is necessary given our legitimate interest in being able to provide and improve the functionalities of the myPOS Service.

- **Geo-location Information**. When you use certain features of the myPOS Platform, we may collect information about your precise or approximate location as determined through data such as your IP address or mobile device's GPS to offer you an improved user experience. Most mobile devices allow you to control or disable the use of location services for applications in the device's settings menu. We may also collect this information even when you are not using the app if this connection is enabled through your settings or device permissions. The legitimate interests that we pursue with this processing is the identification of location-specific problems (i.e. coverage problems for SMS-sending purposes) and other statistical information, which helps us improve our services. This processing is not related to the Location data which we collect for AML/CTF purposes, the latter being mandatory for enrolment.
- **Usage Information**. We collect information about your interactions with myPOS Service such as your usage of any Apps or Functionalities, and other interactions with myPOS Service. The legitimate interests that we pursue with this processing is collection of crash reports and other statistical information, which helps us improve our services.
- **Cookies and Similar Technologies**. We use cookies and other similar technologies, such as web beacons, pixels, and mobile identifiers. We may also allow our business partners to use these tracking technologies on myPOS Service, or engage others to track your behavior on our behalf. While you may disable the usage of cookies through your browser settings, myPOS Platform currently does not respond to a "Do Not Track" signal in the HTTP header from your browser or mobile application due to lack of standardization regarding how that signal should be interpreted. For more information on our use of these technologies, see our Cookies Policy.

Please be advised that when you use myPOS Service, we automatically collect some of the personal information described in the sections above such as **Geo-location Information, Log Data and Device Information, Cookies and Similar Technologies, Payment Transaction Information**.

2. HOW WE USE INFORMATION WE COLLECT

We use, store, and process information, including personal information, about you to provide, understand, improve, and develop myPOS Service, create and maintain a secure environment, pursue our legitimate interests and comply with our legal obligations.

2.1 Providing e-money and payment services.

- initiate a payment, send or request money, acceptance of card payment, funding transaction of your myPOS account;
- authenticate your access to your myPOS Account or your payment instrument;
- communicate with you about your myPOS Account and payment instruments;
- communicate your personal information with third financial institution of Participants in your payment transaction;
- create an account connection between your Account and a third-party account or platform, if applicable;
- perform creditworthiness and other financial standing checks, evaluate applications, and compare information for accuracy and verification purposes

- Detect and prevent fraud, abuse, security incidents, and other harmful activity by blocking myPOS Service or by applying other fraud prevention measures.
- Conduct security investigations and risk assessments.
- Conduct checks against databases and other information sources.
- Comply with legal obligations (such as anti-money laundering regulations).
- Enforce our rights, interests and claims arising from the Legal Agreements.

We process this information given our legitimate interest in improving the myPOS Service and our clients' experience with it, and where it is necessary for the adequate performance of the contract with you as well as to comply with applicable laws.

2.2. Provide, Improve, and Develop the myPOS Service and myPOS Online Store.

- Enable you to access and use the myPOS Service.
- Enable you to communicate with other clients.
- Accept, process and administer online orders for myPOS Terminals;
- Process purchase payments, issue invoices and or other kind of payment documents for the processed order;
- To organize shipment of ordered myPOS Terminal;
- To manage return procedure and refunds for defected devices.
- Operate, protect, improve, and optimize the myPOS Service and your experience, such as by performing analytics and conducting research.
- Provide customer service.
- Send you service or support messages, updates, security alerts, and account notifications.
- If you provide us with your contacts' information, we may process this information: (i) to facilitate your payment transactions, (ii) process your requests, (iii) for fraud detection and prevention, and (iv) for any purpose you authorize at the time of collection.
- To operate, protect, improve, and optimize myPOS Service and experience, and personalize, customize your experience, introduce you to our other Services, we conduct profiling based on your interactions with myPOS Service.

We process this information given our legitimate interest in improving the myPOS Service, and where it is necessary for the adequate performance of the contract with you.

2.3 Create and Maintain a Secure Environment.

- Detect and prevent fraud, spam, abuse, security incidents, and other harmful activity.
- Conduct security investigations and risk assessments.
- Generate one-time permission (OTP) codes for access to myPOS Account and for execution of payment transaction.
- Verify or authenticate information or identifications provided by you.
- Conduct checks against databases and other information third party sources, including background or police checks, data providers, credit bureaus to the extent permitted by applicable laws and with your consent where required.
- Monitor your payment transactions
- Resolve any disputes between you and any of our clients and other users and enforce our agreements with third parties.
- Enforce our legal rights.

We process this information given our legitimate interest in protecting myPOS Service, to measure the adequate performance of our contract with you, and to comply with applicable laws.

2.4. Provide, Personalize, Measure, and Improve our Advertising and Marketing.

- Send you promotional messages, marketing, advertising, and other information related to myPOS Service **and the products and services of unaffiliated businesses** that may be of interest to you based on your preferences and social media advertising through social media platforms such as Facebook, LinkedIn or Google.
- To provide personalised myPOS Services offered by us on third-party websites and online services. We may use your Personal Data and other information collected in accordance with this Privacy Policy to provide a targeted display, feature or offer to you on third-party websites. We may use cookies and other tracking technologies to provide these online services and/or work with other third-parties such as advertising or analytics companies to provide these online services.
- To provide you with location-specific options, functionality or offers if you elect to share your Geolocation Information through the Services. We will use this information to enhance the security of the myPOS Service and provide you with location-based Service, such as advertising, search results, and other personalised content.
- To make it easier for you to find and connect with others, we may use your information you have shared with the

Service to suggest connections between you and people you may know. For example, we may associate information that we learn about you through your and your contacts' use of the Services, and information you and others provide to suggest people you may know or may want to transact with through our Services. Social functionality and features designed to simplify your use of the Services with others vary by Service.
- Personalize, measure, and improve our advertising.
- Administer referral programs, rewards, surveys, sweepstakes, contests, or other promotional activities or events sponsored or managed by us or its third-party partners.
- For participation in games, quizzes and completion of questionnaire or a contest entry form for promotional campaigns.
- Conduct profiling on your characteristics and preferences (based on the information you provide to us, your interactions with myPOS Service, information obtained from third parties) to send you promotional messages, marketing, advertising and other information that we think may be of interest to you.

We will process your personal information for the purposes listed in this section given our legitimate interests in relation to the products we have already offered you and your consent in undertaking marketing activities to offer you products or services that may be of your interest. You have the right to object or opt-out from processing your personal information for the purposes described above by withdrawing your consent at any time and free of charge.

3. WITH WHOM DO WE SHARE PERSONAL DATA

3.1. With other members of the myPOS corporate family: We may share your Personal Data with members of the myPOS Group of companies or within our extended family of companies that are related by common ownership or control, so that we may provide the Services you have requested or authorised or to manage the risk, or to help detect and prevent potentially illegal and fraudulent acts and other violations of our policies and agreements and to help us manage the availability and connectivity of myPOS Services and communications.

3.2. With third part service providers: We may share personal information with third party service providers that support us in providing myPOS Service, products and/or Platform with functions at our decision and our behalf.

These third-party service providers may for example:

- verify your identity or authenticate your identification documents,
- facilitating technically the Video Call and/or store the Video Call recording;
- check information against public databases,
- conduct background or police checks, fraud prevention, and risk assessment,
- perform risk monitoring;
- perform product development, maintenance and debugging,
- allow the provision of myPOS Service through third party platforms and software tools (e.g. through the integration with our APIs), or
- provide customer support,
- IT support and development services;
- card plastic production services;
- resell and distribute myPOS products;
- provide technical support for myPOS products;
- promote myPOS Service as business introducers, distributors, promoters, sales agents or similar;
- perform courier services on our behalf;
- provide cloud, storage or collocations services;
- provide audit and accountancy services;
- provide legal, compliance or other consultancy services;
- Marketing and Public Relations services

These providers have limited access only to your information necessary to perform the tasks for which they were contracted for on our behalf and are contractually bound to protect and to use it only for the purposes for which it was disclosed and consistent with this Privacy Policy.

3.3. With other financial institutions that we have contracted to enable us to provide effectively myPOS Service to our customers: These financial institutions may only use this information in order for us to provide you with the wider scope of payment features. Such may be:

- Correspondent banks for the purposes of settling money transfers and currency exchange operations;
- Domestic payment schemes for the purposes of processing domestic payments;
- International payment schemes for the purposes of processing euro payments;

- Card Organizations for the purposes of card issuing and acquiring;
- Financial Institutions

3.4. With the other parties to transactions when you use myPOS Services, such as other Clients, merchants, and their service providers: We may share information with the other participants to your transactions, including other clients or payers/payees you are sending or receiving funds from, and merchants or their service providers when you use the Services to pay for goods or services. The information includes:

- Personal Data necessary to facilitate the transaction;
- Personal Data to help other participant(s) resolve disputes and detect and prevent fraud; and

3.5. With other third parties for our legitimate interest or as permitted or required by law: We may share information about you with other parties for our legitimate interest or as permitted or required by law, including:

- if we need to do so to comply with a law, legal process or regulations;
- to law enforcement authorities or other government officials, or other third parties pursuant to a subpoena, a court order or other legal process or requirement applicable to us or our corporate family;
- if we believe, in our sole discretion, that the disclosure of Personal Data is necessary or appropriate to prevent physical harm or financial loss or in connection with an investigation of suspected or actual illegal activity;
- to protect the vital interests of a person;
- with credit agencies and data processors for credit reference checks and anti-fraud and compliance purposes;
- to investigate violations of or enforce a user agreement or other legal terms applicable to any Service;
- to protect our property, Services and legal rights;
- to facilitate a purchase or sale of all or part of our business;
- in connection with shipping and related services for purchases made using a Service;
- in relation to promoting myPOS Service to end users by third party business introducers;
- in relation to distribution of myPOS Terminals to end users by third party retailers and distributors.
- to help assess and manage risk and prevent fraud against us, our clients and fraud involving our websites, mobile apps or use of our Services, including fraud that occurs at or involves our business partners, strategic ventures, or other individuals, and merchants;
- to banking partners as required by card association rules for inclusion on their list of terminated merchants;
- to credit reporting and collection agencies;
- to companies that we plan to merge with or be acquired by; and
- to support our audit, compliance, and corporate governance functions.

With your consent: We also will share your Personal Data and other information with your consent or direction, including if you authorise an account connection with a third-party account or platform.

In addition, we may provide aggregated statistical data to third-parties, including other businesses and members of the public, about how, when, and why users visit our website and services. This data will not personally identify you or provide information about your use of myPOS Service. We do not share your Personal Data with third parties for their marketing purposes without your consent.

3.6. Aggregated Data. We may also share aggregated information (information about our users that we combine together so that it no longer identifies or references an individual user) and other anonymized information for regulatory compliance, industry and market analysis, demographic profiling, marketing and advertising, and other business purposes.

3.7 Monitoring

We may monitor or record telephone calls, emails, web chat or other communications with you for regulatory, security, customer services or training purposes. When visiting our offices, CCTV, access control systems and/or other monitoring systems may be in operation.

3.8 Social Media

We may review and use public comments and opinions made on social networking sites (e.g. Facebook and Twitter) to better understand our customers and our provision and development of myPOS Service.

3.9 Business Transfers.

If any of the companies that provides myPOS Services is involved in any merger, acquisition, reorganization, sale of assets, transfer of portfolio, bankruptcy, or insolvency event, then we may sell, transfer or share some or all of our assets, including

your information in connection with such transaction or in contemplation of such transaction (e.g., due diligence). In this event, we will notify you before your personal information is transferred to a different legal person and/or becomes subject to a different privacy policy.

4. Customer Authentication

We may share your personal information iCard Services AD, UIN 175415100, with registered seat and address in Varna, Business Park Varna, B1, Bulgaria and iCard AD, Bulgaria, in relation to the customer two-factor authentication, required under the PSD2 laws, via technical tool Gate Keeper - mobile application that facilitates the strong customer authentication.

5. YOUR RIGHTS

You may exercise any of the rights described in this section before the respective Data Controller pursuant to the Legal Agreements by sending an email from your e-mail registered for myPOS Service to the respective Company providing the Service to you under the respective Legal Agreement stated below. Please note that we may ask you to verify your identity before taking further action on your request. Please note that upon receipt of your e-mail we shall try our best to provide you with the requested information and resolve your request in reasonable time, subject to all obligations which we or the related companies have under the applicable laws.

5.1 Managing Your Information.

You have the right to obtain the following:

- confirmation of whether, and where, the we are processing your personal data;
- information about the purposes of the processing;
- information about the categories of data being processed;
- information about the categories of recipients with whom the data may be shared;
- information about the period for which the data will be stored (or the criteria used to determine that period);
- information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;
- information about the existence of the right to complain to any Regulator;
- where the data was not collected from you, information as to the source of the data; and
- information about the existence of, and an explanation of the logic involved in, any automated processing.
- Additionally, you may request a copy of the personal data being processed.

5.2 Rectification of Inaccurate or Incomplete Information.

You have the right to ask us to correct inaccurate or incomplete personal information concerning you (and which you cannot update yourself via your online access to myPOS Account).

5.3 Data Access and Portability.

You have the right to:

- receive a copy of your personal data in a structured, commonly used, machine-readable format that supports re-use;
- transfer your personal data from one controller to another;
- store your personal data for further personal use on a private device; and
- have your personal data transmitted directly between controllers without hindrance.

In some jurisdictions, applicable law may entitle you to request copies of your personal information held by us.

5.4 Data Retention and Erasure.

We generally retain your personal information for as long as is necessary for the performance of the contract between you and us and to comply with our regulatory obligations. If you no longer want us to use your information to provide myPOS Service to you, you can request that we erase your personal information and close your myPOS Account, providing your account is in good standing, not blocked or somehow limited for compliance, risk or regulatory reasons, or due to your outstanding obligation to us, court order, pledge or order by another regulator or other reason which prevent us by law to close your account or terminate the Service. In case the Data Controller is a regulated financial institution, such as credit institution, E-money institution or similar, such Data Controller is obliged under PSD and AML laws to keep your personal information and all transactions history for a period of 5 years after the termination of the relation with you (or where the laws of the United Kingdom of Great Britain and Northern Ireland are applicable – for a period of 6 years). Please note that if you request the

erasure of your personal information:

- We may retain some of your personal information as necessary for our legitimate business interests, such as fraud detection and prevention and enhancing security. For example, if we suspend a myPOS Account for fraud or safety reasons, we may retain certain information from that myPOS Account to prevent that client from opening a new myPOS Account in the future. We are also obliged to retain personal data which we have collected for the purposes of complying with the relevant anti-money laundering and anti-terrorism financing for a period as defined under the applicable law.
- We may retain and use your personal information to the extent necessary to comply with our legal obligations. For example, myPOS may keep some of your information for tax, legal reporting and auditing obligations.
- Because we maintain the myPOS to protect from accidental or malicious loss and destruction, residual copies of your personal information may not be removed from our backup systems for a limited period of time.

5.5 Withdrawing Consent and Restriction of Processing.

Where you have provided your consent to the processing of your personal information by us you may withdraw your consent at any time by changing your Account settings or by sending a communication to us specifying which consent you are withdrawing. Please note that the withdrawal of your consent does not affect the lawfulness of any processing activities based on such consent before its withdrawal. Additionally, in some jurisdictions, applicable law may give you the right to limit the ways in which we use your personal information, in particular where (i) you contest the accuracy of your personal information; (ii) the processing is unlawful and you oppose the erasure of your personal information; (iii) we no longer need your personal information for the purposes of the processing, but you require the information for the establishment, exercise or defence of legal claims; or (iv) you have objected to the processing and pending the verification whether our legitimate grounds override your own.

5.6 Objection to Processing.

In some jurisdictions, applicable law may entitle you to require us not to process your personal information for certain specific purposes (including profiling for marketing purposes) where such processing is based on legitimate interest. If you object to such processing we will no longer process your personal information for these purposes unless we can demonstrate compelling legitimate grounds for such processing or such processing is required for the establishment, exercise or defence of legal claims. Please note that Data Controllers which are regulated financial institutions, such as credit institutions, E-money institutions or similar are obliged under AML laws to make risk profiling of their customers upon opening of the relationship and constantly during the relationship and this is a legitimate reason. In case you do not wish us to process your personal data for certain specific purposes, which are legitimate purposes to us, you shall have to close your account or we may have to stop providing you some or all of the Services, subject to all conditions for the closing of the account, specified above in this Section.

Where your personal information is processed for direct marketing purposes, you may, at any time ask us to cease processing your data for these direct marketing purposes by sending an e-mail to the contact e-mails below.

5.7 Lodging Complaints.

5.7.1. You should in first place try to resolve the matter by sending an e-mail to the respective Data Controller under this Privacy Policy from your registered e-mail for the Service:

- Where the responsible Data Controller (as outlined in the introduction of the Privacy Policy) is specified to be myPOS Europe Ltd, UK you may contact us at:

Data Protection Officer (DPO):
dpo@mypos.com
myPOS Europe Ltd
The Shard, Level 24
32 London Bridge Street
London,
SE1 9SG

- Where the responsible Data Controller (as outlined in the introduction of the Privacy Policy) is specified to be iCard AD, Bulgaria, you may contact us at:

Data Protection Officer (DPO):
dpo@icard.com

iCARD AD
Business Park Varna No B1, Varna 9023, Bulgaria

- Where the responsible Data Controller (as outlined in the introduction of the Privacy Policy) is specified to be myPOS Services OOD you may contact us at:

Data Protection Officer (DPO):
dpo@mypos.bg
myPOS Services OOD,
Business Park Varna No B1, Varna 9023, Bulgaria

5.7.2 **Competent Regulator**. In case you are not satisfied with the reply or resolution of the respective Data Controller, you have the right to lodge complaints about the data processing activities carried out by us before the competent data protection supervisory authorities as described below.

- If the Data Controller responsible for the respective data processing, subject to your complaint, is myPOS Europe Ltd. UK you have the right to file a complaint with its lead supervisory authority, the Information Commissioners Office, UK:

Address:
Wycliffe House
Water Lane
Willmslow
Cheshire
SK9 5AF
e-mail: casework@ico.org.uk

- If the Data Controller responsible for the respective data processing, subject to your complaint, is iCard AD, Bulgaria you have the right to file a complaint with its lead supervisory authority, Commission for Protection of Personal Data, Bulgaria:

Address:
Sofia 1592
2 Prof. Tsvetan Lazarov blvd.
e-mail: kzld@cpdp.bg

- If the Data Controller responsible for the respective data processing, subject to your complaint, is myPOS Services OOD, Bulgaria you have the right to file a complaint with its lead supervisory authority, the Commission for Protection of Personal Data, Bulgaria:

Address:
Sofia 1592
2 Prof. Tsvetan Lazarov blvd.
e-mail: kzld@cpdp.bg

6. OPERATING GLOBALLY

To facilitate our global operations we may be required to transfer, store, and process your information within our family of companies or with service providers based in Europe, India, Asia Pacific and North and South America. Laws in these countries may differ from the laws applicable to your Country of Residence. For example, information collected within the EEA may be transferred, stored, and processed outside of the EEA for the purposes described in this Privacy Policy. Where we transfer store and process your personal information outside of the EEA we have ensured that appropriate safeguards are in place to ensure an adequate level of data protection.

7. INTERNATIONAL TRANSFERS

7.1 EU-US & Swiss-US Privacy Shield.

Where we disclose any of your collected personal information outside EEA to USA (if applicable), we shall comply with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework and any other adequacy decision.

7.2 Other Means to Ensure an Adequate Level of Data Protection.

In case personal information is shared with corporate affiliates or third-party service providers outside the EEA in absence of an adequacy decision, we have - prior to sharing your information with such corporate affiliate or third-party service provider – established the necessary means to ensure an adequate level of data protection. We will provide further information on the means to ensure an adequate level of data protection on request.

Protection of personal data transferred from or to the United Kingdom of Great Britain and Northern Ireland in the absence of an adequacy decision:

In the absence of an adequacy decision after the United Kingdom of Great Britain and Northern Ireland leaves the European Union, we shall enter into Data processing agreements, including Standard contractual clauses for data transfers between EU and non-EU countries, with our new or existing vendors or similar parties from the United Kingdom of Great Britain and Northern Ireland

8. SECURITY

We take the responsibility to ensure that your personal information is secure, kept in an encrypted form on servers, collocated in Special data centres in Class A jurisdictions in Europe. To prevent unauthorized access or disclosure of information we maintain physical, electronic and procedural safeguards that comply with applicable regulations to guard non-public personal information. Once you are logged into your Account, all internet communication is secured using Secure Socket Layer (SSL) technology with High-grade security Encryption (AES-256, 256 bit keys, certified by StartCom Ltd). We restrict access to your personally identifiable information only to employees who need to know that information in order to provide products or services to you.

If you know or have reason to believe that your myPOS Account credentials have been lost, stolen, misappropriated, or otherwise compromised or in case of any actual or suspected unauthorized use of your myPOS Account, please contact us following the instructions in the Contact Us section below. While we are dedicated to securing our systems and Services, you are responsible for securing and maintaining the privacy of your password(s) and Account/profile registration information and verifying that the Personal Data we maintain about you is accurate and current.

9. Can Children Use Our Services?

myPOS Service is not designed to individuals under the age of 18. We do not knowingly collect information, including Personal Data, from children or other individuals who are not legally able to use myPOS Service. If we obtain actual knowledge that we have collected Personal Data from an individual under the age of 18, we will promptly delete it, unless we are legally obligated to retain such data. Contact us if you believe that we have mistakenly or unintentionally collected information from an individual under the age of 18.

10. CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify this Privacy Policy at any time in accordance with this provision. If we make changes to this Privacy Policy, we will post the revised Privacy Policy on myPOS Platform. If you disagree with the revised Privacy Policy, you may cancel your Account. If you do not cancel your Account before the date the revised Privacy Policy becomes effective, your continued access to or use of myPOS Platform will be subject to the revised Privacy Policy.

11. CONTACT US

If you have any questions or complaints about this Privacy Policy or our information handling practices, you may email us from your registered e-mail for the Services to the e-mails stated above in **Section 4.**