iCard

# iCard and GDPR Compliance

**Our commitment to you and the protection of your data**
As of May 25, 2018, the 'General Data Protection Regulation' or GDPR is enacted across all Member-states of the European Union and the European Economic Area. GDPR aims to harmonize the different data protection laws across the Member-states, leading to more standardized protections for all European citizens. At iCard, we welcome this regulatory change because we have always strived to provide our clients with state-of-the-art protection of their personal data.

**Organizational Readiness at iCard**
The protection of our customers' personal data is of utmost importance to us. For the last several months, we've worked tirelessly to ensure all GDPR compliance requirements were met well in advance.

**Data Protection Officer, Privacy Team and GDPR Training**
All of our employees have undergone GDPR training, overseen by our on-site Privacy Team, Compliance Department and our outside privacy consultants. Each new employee must participate in a mandatory training session related to privacy regulations and best practices. New training sessions are carried out annually thereafter for all employees. We have appointed our Data Protection Officer (DPO), which also acts as the Privacy Team leader, in accordance with the requirements of GDPR.

**Internal policies**
The company's internal policies are updated in accordance with the new GDPR requirements.

**The data we collect**
The personal data we collect and process is described in detail in our Privacy Policy. We process personal data on the basis of different grounds, defined by GDPR – legal obligations, for the purposes of concluding and/or executing a legal relationship, legitimate interest and based on clients' consent.

**How we use the collected data**
We use, store, and process personal information in order to provide, understand, improve, and develop our services, create and maintain a secure environment, pursue our legitimate interests and comply with our legal obligations. For detailed information please check our Privacy Policy.

**Why are we taking pictures of our clients and their ID documents and is it GDPR-compliant?**
In accordance with our legal obligations under the relevant Anti-money laundering and anti-terrorism financing regulations (or AML/CFT laws), we are obliged to verify each of our customer's 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 are bound by the law to identify and verify the owner of the account and since our customers are not always able to upload the required information on their own, we do it instead. In an online environment, we've implemented a video identification chat following the best practices. We do this for our clients' convenience.

The AML/CFT laws, in broad terms, require financial institutions and other entities that are at risk of being used as a tool to launder money or finance terrorism, to:

1) identify their clients, which means that the obliged entity must ask the client to provide his/her personal details.

2) verify their identity, which means that the obliged entity must "check" that the personal details of the person are not falsified, forged, stolen or similar.

When the process above is done on a non-face-to-face principle, such as through an app, we must ensure that the verification of the client's identity must be done with at least two technical measures.

The video-chat functionality and the requirement to take photos of our clients and their ID is at this time the fastest, legal customer-friendly way to provide our services.

**Data Protection Impact Assessment**
We have carried out a detailed review of all our data processing activities, by product and by department. We have analyzed the grounds for processing, retention periods, technical and legal safeguards for our clients' rights and freedoms and we have ensured that any data processing activity that we carry out is 100% compliant with the law.

iCard

**Encryption and storage of personal data**
We take the responsibility to ensure that all personal information is secure, kept in encrypted on servers, collocated in Special data centres in Class A jurisdictions in Europe.

**Our retention periods**
As a financial institution we are obliged under PSD and AML/CFT laws to keep our customers' personal information and all transactions history for a period of 5 years after the termination of the relation with our clients.

**Correction (rectification) of clients' personal data**
Our customers can request from us to correct inaccurate or incomplete personal information via email to dpo@icard.com

**Data Access**
Our clients have the right to receive a copy of the data we hold for them at any time. The request can be sent via e-mail to dpo@icard.com

**Data Deletion**
We generally retain clients' personal information for as long as is necessary for the performance of the contract between them and us and to comply with our regulatory obligations. Our customers can request the closure of their iCard account and the termination of the contract at any time. However, we are going to keep their data for 5 years after the termination in compliance with the law.

In case the regulatory retention periods have expired, we diligently delete clients' personal information from our systems.

For additional information, please check our Privacy Policy.

**Data transfer as our clients' right**
Our clients have the right to receive a copy of their personal data in a structured, commonly used, machine-readable format that supports re-use. They can transfer their personal data from one controller to another and/or have the personal data transmitted directly between controllers without hindrance.

**Consent withdraw and restriction of personal data processing**
Where our clients have provided their consent to the processing of personal information by us, they may withdraw the consent at any time by changing the Account settings or by sending a communication to us specifying which consent they are withdrawing. Please note that the withdrawal of consent does not affect the lawfulness of any processing activities based on such consent before its withdrawal.

**Business accounts**
Please be informed that corporations are not data subjects under GDPR. Business owners who use iCard services and have business accounts can exercise their rights, but only regarding their personal data. The information regarding their company, including its risk profile and due diligence checks is not regulated by GDPR.

**With whom we share personal data**
We may share personal data with members of the iCard Group of companies as we aim to provide the services our clients have requested and in order to help detect and prevent potentially illegal and fraudulent acts and other violations of our policies. We also may share personal information with third party service providers that support us in providing iCard Service, products and/or Platform with functions at our decision and our behalf. For more details, please see section 3 of our Privacy Policy.

**Children and our services**
Our services are not designed to individuals under the age of 18, unless we have expressly specified so in our Privacy Policy or other legal document. 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.

**Clients' personal data after contract/account termination**
Please be aware that we are required by the Payment Services Directive and money laundering legislation to keep each client's data for a period of 5 years after the termination of their contract/account. It is possible certain personal data to be stored for longer periods of time, in case of any court claims and/or other similar procedures, including inquiries, carried out by the competent supervisory authorities.

**Vendor reviews**
All our current vendors have been reviewed to ensure they meet security and privacy requirements defined by GDPR. To maintain assurance, these reviews will be conducted for all incoming vendors. Where we transfer, store and process personal information outside of the European Economic Area we guarantee that appropriate safeguards are in place to ensure an adequate level of data protection.

iCard

Where we deal with entities outside the EEA, we always require our vendors to be either registered under Privacy Shield mechanisms (or similar) or to provide us with a review of their appropriate privacy safeguards.

**Incident response**
Our Incident Response procedures have been designed and tested to ensure potential security events are identified and reported to appropriate personnel for resolution, personnel follow defined protocols for resolving security events, and steps for resolution are documented and reviewed by our Security Team on a regular basis. Additionally, we have updated these policies and procedures to include breach notification if and when a security incident involves the loss of or unauthorized use of personal identifiable information (PII).

**Cookies Compliance**
We use “cookies” and other technologies when users visit or use our websites or mobile apps. This use is based on consent. If our users wish to withdraw their agreement to accept cookies and similar technologies, they can delete the cookies via the browser settings (it is explained how to do so in our Cookies Policy). Please find further information on deleting and blocking cookies at http://www.aboutcookies.org/how-to-delete-cookies/

**Our licenses and registrations**
iCard is registered as an electronic money institution under PSD2 licensed by Bulgarian National Bank, license number 4703-5081, Principle Member of MasterCard, VISA, JCB, AMEX, UnionPay, Bancontact, Borica and other payment schemes.

We provide financial services in the entire EU and EEA. You can find our registration number in the relevant payment infrastructure supervisory authority, i.e. in the United Kingdom you can find us in the Financial Services Register, at: https://register.fca.org.uk/shpo_searchresultspage?search=icard&TOKEN=3wq1nht7eg7tr