

Principles of processing Personal data

# Crip2Card

Valid from 01 of October 2018  
Ver.1

The principles how CRIP2CARD processes personal data are described in these Principles of processing Personal data, hereinafter also referred as the Principles,

The Principles apply if a Client uses, has used or has expressed an intention to use or is in other way related to any of the services provided by CRIP2CARD, including to the relationship with the Client established before these Principles entered into force.

## **1. Definitions**

**Client** - means any natural person who uses, has used or has expressed a wish to use or is in other way related to any of the services provided by CRIP2CARD.

**Personal data** - means any information directly or indirectly related to the Client.

**Processing** - means any operation carried out with Personal data (incl. collection, recording, storing, alteration, grant of access to, making enquiries, transfer, etc.).

**CRIP2CARD** - Exchange service registered in Estonia, whose registered office is in Estonia and who is acting as a controller of Personal data.

## **2. General provisions**

2.1. These Principles describe how CRIP2CARD Processes Personal data on a general level. Specific details on the Processing of Personal data might be also described in agreements, other service related documents and on CRIP2CARD website: <https://crip2card.com>

2.2. CRIP2CARD ensures, within the framework of applicable law, the confidentiality of Personal data and has implemented appropriate technical and organizational measures to safeguard Personal data from unauthorized access, unlawful Processing or disclosure, accidental loss, modification or destruction.

2.3. CRIP2CARD may use authorized processors for Processing Personal data. In such cases, CRIP2CARD takes needed steps to ensure that such data processors Process Personal data under the instructions of CRIP2CARD and in compliance with applicable law and requires adequate security measures.

2.4. CRIP2CARD cookie policies are available on CRIP2CARD website: <https://crip2card.com>

## **3. Categories of Personal data**

3.1. Personal data may be collected from the Client, from the Client's use of the services and from external sources such as public and private registers or other third parties. Personal data categories which CRIP2CARD primarily, but not only, collects and processes are:

3.2. Identification data such as name, personal identification code, date of birth, data regarding the identification document (such as copy of the passport, ID card, driver license). Contact data such as address (such as utility bill, phone bill), telephone number, email address, language of communication. Family data such as information about Client's family, heirs and other related person's.

3.3. Data about the relationships with legal entities such as data submitted by the Client or obtained from public registers or through third party for the execution of transactions on behalf of the legal entity in question. Professional data such as educational or professional career. Financial data such as accounts, ownership, transactions, credits, income, liabilities or executed transactions in exchange service.

3.4. Data on origin of assets or wealth such as data regarding the Client's transaction partners and business activities. Data about trustworthiness and due diligence such as data about payment behavior, damage caused to CRIP2CARD or any third party, data that enables CRIP2CARD to perform its due diligence measures regarding money laundering and terrorist financing prevention and to ensure the compliance with international sanctions, including the purpose of the business relationship and whether the Client is a politically exposed person.

Data obtained and/or created while performing an obligation arising from law- such as data resulting from enquiries made by investigative bodies, notaries, tax administrator, courts and bailiffs, details of income,

credit commitments, property holdings, remarks, historical remarks and debt balances. Data about the Client's tax residency such as data about the country of residence, tax identification number, citizenship.

3.5. Communication data collected when the communicates with CRIP2CARD via telephone, visual and/or audio recordings, e-mail, messages and other communication mechanisms such as social media, data related to the Client's visit at CRIP2CARD web sites or communicating through other CRIP2CARD channels (such as personal cabinet and social networks). Data related to the services such as the performance of the agreements or the failure thereof, executed transactions, concluded and expired agreements, submitted applications, requests and complaints, interests and service fees. Data about habits, preferences and satisfaction such as the activeness of using the services, services used, personal settings, survey responses. Client satisfaction. Data about participation in campaigns such as the points gained.

3.6. Special categories of data such as a Client's health.

#### **4. Purposes and basis of Processing Personal data**

4.1. CRIP2CARD processes Personal data primarily to:

4.1.1. To conclude and execute an agreement, for example a transaction, with the Client, keeping data updated and correct by verifying and enriching data through external and internal sources based on performance of an agreement or in order to take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation.

4.1.2. To protect the interests of the Client and/or CRIP2CARD and examine the quality of services provided by CRIP2CARD and for the purpose of providing proof of a commercial transaction or of other business communication based on: performance of an agreement or in order to take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation or consent from the Client or CRIP2CARD legitimate interests to prevent, limit and investigate any misuse or unlawful use or disturbance of CRIP2CARD services and products, internal training or quality assurance of services. To guarantee the security of CRIP2CARD and/or the Client, protect life and health of the Client and his/her representatives and other rights of CRIP2CARD and the Client based on CRIP2CARD legitimate interest to protect its Clients, employees, visitors and theirs and CRIP2CARD assets.

4.1.3. Offer to the Client the services of CRIP2CARD or carefully selected cooperation partners, including personalized offers, based on consent from the Client or CRIP2CARD legitimate interest to offer additional services. Perform Client surveys, market analyses and statistics; organize campaigns for a Client based on CRIP2CARD legitimate interest to improve CRIP2CARD services, improve the Client's user experience of services and to develop new products and services or consent from the Client.

4.1.4. To comply with applicable law and international agreements, for example related to implementing the "customer due diligence" and "know your customer", prevent, discover, investigate and report potential money laundering, terrorist financing, if the Client is subject to financial sanctions or is a politically exposed person and to verify identity based on performance of an agreement or in order to take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation or CRIP2CARD legitimate interest for a sound risk management and corporate governance.

4.1.5. To authorize and control access to and functioning of digital channels, prevent unauthorized access and misuse of those and to ensure the safety of information based on performance of an agreement or take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation or consent from the Client or CRIP2CARD legitimate interests to have control over authorizations, access to and functioning of CRIP2CARD digital services.

Improve technical systems, IT-infrastructure, customizing the display of the service to the device and to develop CRIP2CARD services such as by testing and improving technical systems and IT-infrastructure based on CRIP2CARD legitimate interests to improve technical systems and IT-infrastructure.

4.1.6. To establish, exercise, assign and defend legal claims based on performance of an agreement or in order to take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation or CRIP2CARD legitimate interests to exercising legal claims.

4.1.7. To fulfil obligations to execute international transactions via credit institutions and domestic payments via domestic, European and international payment systems and to comply with rules and obligations defined in, amongst others card- and security related, European and international standards and certification schemes based on performance of an agreement or take steps at the request of the Client prior to entering into an agreement or compliance with a legal obligation.

## **5. Profiling, personalized offering and automated decision making**

5.1. Profiling refers to the automatic Processing of Personal data used to assess certain personal characteristics of a Client in particular to analyze or predict, for example, the economic situation, personal preferences, interests, place of residence of such individual. Profiling is used to make analysis for Client advice, direct marketing purposes, for automated decision-making such as credit assessments, for risk management, for insurance underwriting and for transaction monitoring to counter fraud and is based on CRIP2CARD legitimate interest, compliance with a legal obligation, performance of an agreement or consent from the Client.

5.2. CRIP2CARD may process Personal data to improve the Client's user experience of the digital services, such as customizing the display of the services to the device used and creating suitable offers for Clients. Unless direct marketing has been restricted by the Client, CRIP2CARD may process Personal data for the purpose of providing general and personalized offers of CRIP2CARD services. Such marketing may be based on services the Client uses and on how the Client uses the services, and on how the Client navigates in digital channels of CRIP2CARD.

5.3. For personal offering and marketing based profiling, which is done according to CRIP2CARD legitimate interest, CRIP2CARD ensures that Clients can make their choices and use a convenient tool to manage their privacy settings.

5.4. CRIP2CARD may also collect statistical data regarding the Client, such as typical behavior and lifestyle patterns based on demographic household data. Statistical data for creating segments/profiles can be collected from external sources and may be combined with CRIP2CARD internal data.

## **6. Recipients of Personal data**

6.1. Personal data is shared with other recipients, such as:

6.1.1. Authorities (such as law enforcement authorities, bailiffs, notary offices, tax authorities, supervision authorities and financial intelligence units).

6.1.2. Legal entities in CRIP2CARD (eWalletex LTD OU, Estonia).

6.1.3. Credit and financial institutions, insurance service providers and intermediaries of financial services, third parties participating in the trade execution, settlement and reporting cycle.

6.1.4. Auditors, legal and financial consultants, or any other processor authorized by CRIP2CARD.

6.1.5. Third parties maintaining registers (such as to credit registers, population registers, commercial registers, securities registers or other registers holding or intermediating Personal data).

6.1.6. Participants and/or parties related to domestic, European and international payment systems, such as SWIFT.

6.1.7. Other persons related to provision of services of CRIP2CARD such as providers of archiving, postal services, providers of services rendered to the Client.

## **7. Geographical area of Processing**

7.1. As a general rule the Personal data is processed within the European Union/European Economic Area (EU/EEA) but in some cases transferred and processed to countries outside the EU/EEA.

7.2. Transfer and Processing of Personal data outside the EU/EEA can take place provided there is a legal

ground, i.e. legal requirement conclusion or performance of an agreement or Client's consent and appropriate safeguards are in place. Appropriate safeguards, such as:

- There is an agreement in place including the EU Standard Contractual Clauses or other approved clauses code of conducts, certifications etc., approved in accordance with the General Data Protection Regulation;
- The country outside of the EU/EEA where the recipient is located has adequate level of data protection as decided by the EU Commission;
- The recipient is certified under the Privacy shield (applies to recipients located in the United States).

7.3. Upon request the Client can receive further details on Personal data transfers to countries outside the EU/EEA.

## **8. Retention periods**

8.1. Personal data will be processed no longer than necessary. The retention period may be based on agreements with the Client, the legitimate interest of CRIP2CARD or applicable law (such as laws related to bookkeeping, anti-money laundering, statute of limitations, civil law, etc.).

## **9. Clients' rights as a data subject**

A Client (data subject) has rights regarding his/her data Processing that is classified as Personal data under applicable law. Such rights are in general to:

9.1. Require his/her Personal data to be corrected if it is inadequate, incomplete or incorrect.

9.2. Object to Processing of his/her Personal data, if the use of Personal Data is based on a legitimate interest, including profiling for direct marketing purposes (such as receiving marketing offers or participating in surveys).

9.3. Require the erasure of his/her Personal data, for example, that is being processed based on the consent, if he/she has withdrawn the consent. Such right does not apply if Personal data requested to be erased is being processed also based on other legal grounds such as agreement or obligations based on applicable law.

9.4. Restrict the Processing of his/her Personal data under applicable law, e.g. during the time when CRIP2CARD assesses whether the client is entitled to have his/her data erased.

9.5. Receive information if his/her Personal data is being processed by CRIP2CARD and if so then to access it.

9.6. Receive his/her Personal data that is provided by him/herself and is being processed based on consent or in order to perform an agreement in written or commonly used electronic format and were feasible transmit such data to another service provider (data portability).

9.7. Withdraw his/her consent to process his/her Personal data.

9.8. Not to be subject to fully automated decision-making, including profiling, if such decision-making has legal effects or similarly significantly affects the Client. This right does not apply if the decision-making is necessary in order to enter into or to perform an agreement with the Client, if the decision-making is permitted under applicable law or if the Client has provided his/her explicit consent.

9.9. Lodge complaints pertaining to the use of Personal data to the Data Protection Authority at <https://vwww.dvi.gov.lv> if he/she considers that Processing of his/her Personal data infringes his/her rights and interests under applicable law.

## **10. Contact details**

10.1. Clients may contact CRIP2CARD with any enquiries, withdrawal of consents, requests to exercise data subject rights and complaints regarding the use of Personal data.

10.2. Contact details of CRIP2CARD are available on CRIP2CARD website <https://crip2card.com>

10.3. Contact details of the appointed Data Protection Officer: [dataprotection@crip2card.com](mailto:dataprotection@crip2card.com)

### **11. Validity and amendments of the principles**

11.1 The principles are provided to the Clients on <https://crip2card.com>

11.2 CRIP2CARD is entitled to unilaterally amend the principles at any time, in compliance with the applicable law, by notifying the Client of any amendments via website of CRIP2CARD, via e-mails or personal cabinet messages or in another manner (for example through mass media), not later than one month prior to the amendments entering into force.