H-1117 Budapest,
Infopark „I" épület
Infopark sétány 1.
tel: +36 (1) 464-7099
fax: +36 (1) 464-7080
hello@barion.com
www.barion.com

Data Protection Policy

of Barion Payment Inc.

Effective date: October 1st, 2015

Information about the document	
Issued on:	10/01/2015
Valid until:	withdrawal

Approved	
Chief Executive Officer	
Compliance Officer	

Table of contents

1. Policy background

The amendment of the Policy was necessitated by the fact that Barion Payment Inc. is spun off from Sense/Net Zrt. as of 9/30/2015 and will carry on with the electronic money issuing activity, including data management, from October 1st, 2015 on.

2. Objective of the Policy

The objective of this Policy is to ensure compliance with the constitutional principles of data protection principles, the right to informational self-determination, the requirements for data protection and the provisions of the Info Act, including the legislative principles of data protection (Data management principles).

In order to ensure this, this Policy sets out the general framework for managing and destroying the data falling within the scope of the personal data, payment secrets and trade secrets created during or used in connection with the operation of Barion Payment Inc. (hereinafter "the Issuer"), regardless of their presentation.

The guidelines in this Policy and the Data management principles must also be integrated into each process and reflected during process control. Rules for data security and data protection are integrated into the Policies applicable to each function within the Issuer, including, in particular, IT security, compliance and user complaint handling. This Policy establishes the framework for data management and data protection within the Issuer.

3. Definitions

"Business secret" (as defined by Section 2:47 (1) of the Civil Code) means any facts, information, other data and their sets related to an economic activity, which are not generally known or easily accessible for the persons performing the relevant economic activity and whose acquisition, use, disclosure to others or publication by unauthorized persons would prejudice or jeopardize the right holder's legitimate financial, economic or market interests, provided that the right holder lawfully in control of the secret is not imputable with regard to keeping such secret.

"Consent" means a voluntary and explicit expression of the Data Subject's intent based on appropriate information, by which the Data Subject unambiguously agrees to the management of the personal data relating to the Data Subject in full or for certain operations.

"Custodian" means a person who manages a function where data are created, qualifies the Data created and is responsible for the management of the Data s/he qualified. In any case, this is a person directly responsible for the activity during which the data are created, in accordance with the Bylaws of Barion Payment Inc.

"Data management principles":

- Personal data may only be handled for a specific purpose, that is, for exercising rights or fulfilling obligations. Data management must be appropriate to its purpose in all phases; data must be collected and managed fairly and lawfully.
- Only such personal data may be managed that is absolutely necessary for achieving the purpose of data handling and that is suitable for achieving this

purpose. Personal data may only be processed to the extent and for the period required for achieving the specific purpose.

- In the course of data management, such data shall be considered as personal so long as their connection to the data subject can be identified. The connection to the data subject can be reestablished if the data manager has the technical means to reestablish such connection.
- During data management, it must be ensured that data are accurate, complete and, if needed with a view to the purpose of data management, up-to-date and the data subject can only be identified for the period required for achieving the purpose of data management.

"Data management" means any operation or set of operations carried out on data, regardless of the procedure employed, including, but not limited to, the collection, capturing, recording, organization, storage, modification, use, transmission, disclosure, reconciliation or linking, blocking, deletion and destroying and preventing further use of data. It is also considered data management to take photographs, make audio or video recordings or recording physical characteristics enabling the identification of a person (e.g. fingerprints, palm prints, DNA sample, iris image).

"Data manager" means the Issuer. The data manager defines the purpose of data management, makes and implements decisions on data management (including the means used) or ensures that the data processor implements them.

"Data subject" means any specific natural person identified or directly or indirectly identifiable on the basis of personal data.

"Data" means data considered as Strictly Confidential, Confidential, Internal or Public in respect of this Policy.

"Objection" means a declaration made by the Data Subject objecting to the management of the Data Subject's Personal Data and requesting the termination of data management and the deletion of the managed data.

"Payment secret" (as defined by Section 59 of the Payment Services Act) means any facts, information, solutions or data about the User's person, data, financial situation, business activities, finances, ownership and business relationships and contracts concluded with the Issuer, available to the Issuer as an electronic money issuer entity regarding each user in connection with the provision of the payment service involving electronic money. The rules set out in the Credit Institutions Act as to bank secrets must be apply to payment secrets as appropriate, it being understood that "bank secret" in the Credit Institutions Act is replaced by "payment secret" as appropriate.

"Personal data" means any data relating to the Data Subject as well as any conclusion with respect to the Data Subject which can be drawn from such data. In the course of data management, such data shall be considered as personal so long as their connection to the data subject can be identified. A person is considered identifiable especially when the person can be identified, either directly or indirectly, on the basis of name, identifier and/or one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identity.

"Protected data" means Strictly confidential data, Confidential data and Internal data in respect of this Policy. Personal data, Sensitive data, Payment secrets and Business secrets are considered Protected data in any case.

"Sensitive data" means data concerning racial origin, national or ethnic minority background, political opinion or party affiliation, religious or other philosophical beliefs, trade-union membership, health, addictions, sex life, as well as criminal personal data (personal data associated with the Data Subject and concerning criminal records, created by bodies empowered to prosecute

and investigate offences in connection with such offences or prosecution during or before criminal proceedings and within the penal system).

4. Scope of the Policy

4.1. Material scope

The material scope of the Policy covers all Data managed by the Issuer.

4.2. Personal scope

The personal scope of the Policy covers all employees of the Issuer, members of its Supervisory Board and any other person engaged in any other legal relationship involving work and is also applicable to the contract concluded with the Issuer's suppliers if data management, data processing or data transmission is concerned.

5. Duties related to data protection within the Issuer

5.1. Data Protection Officer

5.1.1. Duties of the Data Protection Officer

The duties of the Data Protection Officer include:

a) Being involved in making decisions concerning data management and contributing to guaranteeing data subjects' rights;

b) Drawing up the data protection and data security policy and ensuring that the requirements included therein are met;

c) Monitoring compliance with the provisions of the Act and other legislation on data management as well as internal data protection and data security policies, along with data security requirements;

d) Investigating reports received concerning data protection and, if unauthorized data management is identified, advising the relevant Business unit on proper procedure;

e) Providing advice regarding issues arising in connection with the security of payment secrets and personal data;

f) Keeping the internal data protection records;

g) Ensuring that data protection education is provided;

h) Communicating with Supervisory Bodies or other authorities concerning affairs falling within the Data Protection Officer's scope of duties.

The Data Protection Officer monitors compliance with the provisions of the legislation on data protection, the Data Protection Policy and any other relevant internal policies. If the Data Protection Officer identifies an infringement or unauthorized data management during the Data Protection Officer's activities, the Data Protection Officer will call on the Custodian, data processor or other person that came into contact with the data to cease such infringement or unauthorized data management.

The Data Protection Officer ensures that compulsory data protection education is provided within the Issuer once a year to the Issuer's employees.

The Data Protection Officer keeps the internal data protection records and the associated data transmission records based on the records provided to the Data Protection Officer by the Custodians.

5.1.2. Appointment of the Data Protection Officer and revocation of the appointment

The Data Protection Officer is appointed by the Chief Executive Officer. The appointment is valid until revoked or the termination of the appointed employee's employment.

5.2. The Custodian

5.2.1. Duties of the Custodian

Custodians are responsible for classifying the data created during the fulfillment of the duties of their function, keeping records of them and monitoring that only the persons/organizations authorized to do so in advance by the Custodian can have access to them. The principle to be applied when authorizing access is that those performing data management operations should be provided access to the data to the extent necessary and sufficient for that purpose. In doing so, Custodians must comply with the provisions of the Information Security Policy.

Custodians must continuously monitor the records (data inventory and data transmission records) they keep and notify the Data Protection Officer of any changes in them.

The Data Protection Officer and the Internal Controller are responsible for verifying that the Data are classified appropriately and managed in accordance with their classification.

5.2.2. Responsibilities of the Custodian

By properly regulating and organizing workflows, Custodians must ensure that:

- employees, those engaged in any other legal relationship involving work, suppliers, etc., only obtain Protected Data to the extent necessary to carry their duties,
- the risk of Protected data being obtained by unauthorized third parties is minimized,
- data management and data backup activities and their processes take place in compliance with the relevant data protection legislation and the Issuer's policies.

5.2.3. Appointment of the Custodian and revocation of the appointment

Heads of the Issuer's organizational units set out in the current Bylaws are Custodians in respect of the Data created during the fulfillment of the duties of the organizational units under such Heads' control.

Custodians are not appointed specifically; rather, in any case, the Custodian will be the person directly responsible for the activity during which the data are created, in accordance with the Bylaws of Barion Payment Inc.

6. Classification of data

Strictly confidential: any data classified as such by the Issuer subject to the Issuer's legal obligation or business interests and the disclosure of which would cause the Issuer significant material loss or damage to the Issuer's reputation. The scope of access to Strictly confidential data must be precisely defined by the Issuer. Strictly confidential data are data which, according to the Information security risk matrix, have a rating of 18-27.

Confidential: any data that are not classified as Strictly confidential, but only accessible to the Issuer's employees who need such confidential data for their work. This includes Protected data and any other data that would cause the Issuer significant material loss or damage to the Issuer's reputation. Confidential data are data which, according to the Information security risk matrix, have a rating of 5-17.

Internal: this category includes data which are only accessible to the Issuer's employees or other persons engaged by the Issuer in any other legal relationship involving work or contractual relationship, but would not cause the Issuer significant material loss or damage to the Issuer's reputation if disclosed. Internal data are data which, according to the Information security risk matrix, have a rating of 1-4.

Public: the scope of data available to anyone. The disclosure of or access by persons other than the Issuer to such data does not prejudice the Issuer's business interests. From the data created within the Issuer, this category includes approved marketing materials and communications. Public data are data which are not covered by the data assessment according to the Information security risk matrix, i.e. not classified as Strictly confidential, Confidential or Internal data.

The above list must be used for Data presented either in electronic or in paper form.

7. General rules for Data management

7.1. Management of personal data

Personal data may be managed by the Issuer if necessary for the activity of the Issuer, the Data Subject agreed to it in writing or required by law.

In a procedure launched at the request of the Data Subject (typically the User), it must be presumed that the User agreed to the management of the necessary User data. This must be pointed out to the Data Subject.

Personal data may also be managed if it is not possible to obtain the Data Subject's consent or it would entail disproportionately high costs and the management of personal data:

a) is necessary to fulfill a legal obligation of the Issuer as data manager, or

b) is necessary to uphold the legitimate interests of the Issuer as data manager or a third party, and the upholding of these interests is proportionate to the restriction on the right to the protection of personal data.

Personal data may also be managed in cases other than those described above (e.g. direct marketing) subject to an authorization provided by the Data Subject explicitly to that effect.

7.2. Management of Protected data

Protected data may only be managed within the Issuer if necessary for the activity of the Issuer and the Data Subject agreed to it in writing and/or required by law. Detailed rules for rating and managing Protected data, along with the rating of each type of data according to Section 6 of this Policy, are included in the Information Security Policy along.

7.2.1. Data management in the case of hard copies

Documents containing Protected data must be managed so as to ensure that unauthorized persons do not have access to them. Documents containing Protected data must not be left unattended without locking them away first and must be locked away properly after work.

7.2.2. Data management in the case of electronic media

When managing electronic media containing Protected data, it must be ensured that unauthorized persons do not have access to them. Electronic media containing Protected data must not be left unattended without locking them away first and must be locked away after work.

7.2.3. Management of electronic data

Electronic data may only be transmitted to organizational units performing duties necessary to the operation of the Issuer, to the extent and for the period required for carrying out such duties.

7.2.4. Destruction of the media containing the data

In accordance with the Issuer's current policy on records management, the media containing the data must be disposed of or its content deleted in a way that prevents the data content off the media from being restored by any means (physical destruction, shredding, demagnetization in the case of magnetic or optical media or multiple overwriting passes, etc.). Reports must be drawn up about disposed and destroyed media. Destruction is only possible if the mandatory retention period for data storage required by law has elapsed.

The paper waste created during the preparation of the document containing the data which can be used to retrieve the data must be destroyed with a shredding machine immediately after use.

8. Data management provisions for the Issuer's employees

8.1. Obligations of the Issuer's employees

Persons having an employment relationship or any other relationship involving work with the Issuer (hereinafter "Employees") must become familiar with this Policy at the date of the commencement of employment, but not later than on their first day of work.

The Issuer's employees are required to retain the Protected data disclosed to them and ensure that such data are not disclosed to or obtained by unauthorized third parties. In their work, employees must pay attention to the proper management of paper or electronic documents containing Protected data. If they discover that

the Protected data were disclosed to or obtained by unauthorized third parties, they must inform the Data Protection Officer immediately.

The Issuer's employees must act as instructed by the Data Protection Officer during the procedure initiated by the Data Protection Officer.

8.2. Confidentiality

Any person having access to the Protected data must keep such data confidential indefinitely and ensure that the Protected data are not disclosed to third parties or become accessible, except in the cases specified by law, this Policy and the applicable legislation.

Statistical data about the Issuer based on, but not disclosing, Personal data may be provided.

After the purpose of the data management has ceased, the data must be deleted if their retention is not required by law.

8.3. Specific rules for managing data about the Issuer's employees

8.3.1. Management of personal and sensitive data of the Issuer's employees

Special attention must be paid when managing Personal data obtained by the Issuer as employer about its employees during the exercise of employer's rights. The Issuer does not manage Sensitive data about their employees, save for the exceptions listed. The Issuer is only entitled to manage Sensitive data as a result of the Issuer's rights as employer (e.g. requiring an extract from a judicial record, sick leave, putting on sick pay) in respect of the relevant data. If Sensitive data are accidentally obtained by the Issuer, the Issuer will cease to manage such data without delay.

8.3.2. The range of key data managed by the Issuer about the employees

- Data managed in connection with the employment of the employees (employment contract, relevant documents, evidence of qualifications, documentation related to payroll, etc.). Data managed in connection with certain official procedures, documents obtained by the Issuer (e.g. extract from a judicial record, other declarations).
- If the Issuer's employees are also the Issuer's users, the range of data and documents obtained by the Issuer on the basis of that legal relationship.
- The data obtained by the Issuer during the work performed by the employees, information recorded through the use of computers, internet, telephone and passes by employees and data recorded by the Issuer's security system and cameras.
- Data managed in connection this the Issuer's prudent operation in compliance with the legislation (compliance statements, etc.).

8.3.3. Rules for managing the data of the Issuer's employees

During the management of the data about the Issuer's employees by the Issuer, it must be ensured that such data are only managed by any employee whose data management is absolutely necessary for certain necessary operations.

If the management of data about the Issuer's employees are not necessary for the employees to perform their duties, such data may not be disclosed to other employees.

The Chief Executive Officer is considered a person who requires all the data managed by the Issuer for carrying out the CEO's duties.

The Issuer's Internal Controller and the Data Protection Officer are entitled to have access to the data of the Issuer's employees to the extent required for the performance of their duties.

9. Rules for transmitting Protected data to third parties

9.1. Basis for transmitting Protected data outside the Issuer

Protected data may only be disclosed to third parties if:

a) the Data Subject or the Data Subject's legal representative requests or authorizes the data to be disclosed, clearly indicating the scope of secrets concerning the Data Subject that may be disclosed (in such cases)

b) an exemption to the obligation of secrecy is provided by law; or

c) with regard to Payment secrets, the Issuer's interest makes it necessary to sell a claim on the Data Subject or enforce an overdue claim.

9.2. Procedure to be followed when transmitting state secrets, professional secrets and data indicating money-laundering

The Issuer does not manage any state secrets or professional secrets.

When data, facts or circumstances indicating money-laundering arise, the provisions of the Issuer's Money-Laundering Policy must be applied.

9.3. Data transmission abroad

The Issuer may transmit Personal data to a data manager conducting data management in a third country or a data processor conducting data processing in a third country if:

a) the Data Subject has agreed to it, or

b) the conditions for data management set out in the Info Act are met and an adequate level of protection is ensured for Personal data in the third country during the management or processing of such transmitted data.

An adequate level of protection for personal data is ensured if:

a) it is established by a binding act of the European Union, or

b) there is an international treaty in effect between the third country and Hungary containing rules guaranteeing that the Data Subjects' rights provided for in the Info Act are enforced, a right to appeal is ensured and data management and/or data processing are independently controlled.

Data transmission to a state which is a party to the Agreement on the European Economic Area is considered as if data transmission took place in Hungary.

9.4. Rules for transmitting data to the Issuer's suppliers

When concluding contracts with suppliers, the Issuer ensures that the contract to be concluded complies with this Policy, provided that data management or data transmission is to take place.

9.5. Rules for outsourcing

The Issuer may outsource activities related to issuing electronic money and providing a payment service on the condition that the data protection regulations as well as the relevant provisions of Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises and Act CCXXXV of 2013 on Payment Service Providers are complied with.

10. Data protection register

In order to fulfill its obligation, the Issuer as data manager requested to be entered in the data management register maintained by the Hungarian National Authority for Data Protection and Freedom of Information.

The Issuer's data management registration number: NAIH-73794/2014.

11. Right to object and raise complaint

General rules

At the Data Subject's written request:

- the Issuer will provide the Data Subject, in writing, with the data kept on record, managed and transmitted in respect of the Data Subject, indicating their source as well as the objective, legal basis and duration of the data processing, in accordance with existing legislation.
- the Issuer, when using a data processor, will inform the Data Subject about the data processor's name, address and data processing-related activities, and, if the Data Subject's personal data are transferred, the legal basis and the recipient of the transfer. The Issuer will provide the requested information in writing within 30 days of the submission of the request.

In the instances provided for by law, the Issuer may refuse to provide information to the Data Subject. If information provision is refused, the Data Subject may apply to a court or the Hungarian National Authority for Data Protection and Freedom of Information.

At the Data Subject's request, the Issuer will correct or, in cases specified by law, delete any incorrect personal data made available to the Issuer. Instead of deleting, the Issuer may block personal information if so requested by the Data Subject or it can be assumed on the basis of the available information that deletion would prejudice the legitimate interests of the Data Subject. The Issuer will notify the Data Subject and/or any additional data processors about the correction, blocking, marking and deletion if failure to give notification would prejudice the legitimate interests of the Data Subject with regard to the purpose of data management.

If the Issuer does not comply with the Data Subject's request for correction, blocking or deletion, the Issuer will provide the reasons in fact and in law for refusing the request in writing within 30 days of the receipt of the request.

If the request is refused and/or the Issuer fails to meet the above deadline, the Data Subject may apply to a court or the Hungarian National Authority for Data Protection and Freedom of Information.

Rules of the procedure within the Issuer

If the Issuer's User, employee or other person or authority objects to the management of their Protected data or lodges a complaint about the method of data management, the Data Protection Officer must address such objection or complaint as soon as possible after the submission of the request, but no later than within the period specified in the Issuer's current policy for handling complaints.

If the Custodian or the Data Manager did not manage the data as required by law or by this Policy, the Data Protection Officer would investigate the complaint or instruct the Custodian to conduct the investigation, involving the Head of IT Security and/or the Internal Controller when necessary. In such case, the Custodian will inform the Data Protection Officer about the result of the investigation.

The Data Protection Officer will inform the applicant about the result of the investigation. If the objection or complaint is valid, the Data Protection Officer will arrange for the data management (including additional data collection and data transmission) to cease and the data to be deleted. The Data Protection Officer notifies about the objection, complaint and the measures taken in response all those to whom the Issuer previously transmitted the Protected data concerned and who will be required to arrange for the enforcement of the right to object and raise complaint.

12. Control

Compliance with requirements concerning data protection, in particular the provisions of this Policy, will be verified by Custodians as well as the Data Protection Officer and the Internal Controller as part of internal control activities.

13. Legislation and policies relevant to the Policy

Relevant legislation:

Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Info Act)

Act V of 2013 on the Civil Code (Civil Code)

Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (Credit Institutions Act)

Act CCXXXV of 2013 on Payment Service Providers

Act CLV of 2009 on the Protection of Classified Data

Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing