SECURITY PRINCIPLES AT LOYALTY PARTNER POLSKA SP. Z O. O.

Introduction

This document was created based on the provisions contained in the security policy of Loyalty Partner Poland Sp. z o.o. and those derived from the rules of use of the IT system (document "IT Terms of Use" available on the LP intranet). Its purpose is to set standards of conduct in the use of LP infrastructure (in particular, how to safely use e-mail, network, computer equipment) and to define the basic principles on which personal data are processed/accessed.

Personal Data Administrator, Data Protection Officer

Personal Data Administrator ("ADO")- the entity or person who decides on the purposes and means of personal data processing. ADO is understood to mean **Loyalty Partner Polska Sp. z o.o. ("LP")**.

Data Protection Inspector ("DPO") - a person appointed by the ADO who is responsible for ensuring data processing in accordance with the relevant provisions of the Act and the law. At Loyalty Partner Polska Sp. z o.o., the function of the **DPO** is performed by **Dariusz Sadowski** (mojedane@payback.net / dariusz.sadowski@payback.net).

The LP has appointed and reported to the register maintained by the Office of Personal Data Protection a DPO who is responsible for overseeing and verifying that data processing by the ADO and its employees complies with data protection laws, including the General Data Protection Regulation ("**GDPR**"), national laws and the ADO's internal policies

IOD in particular:

- Informs the ADO, entities processing personal data on behalf of the ADO, and employees who process personal data about their obligations under data protection laws and advises them accordingly.
- Monitors compliance with data protection laws and policies of the ADO or processor in the area of personal data protection, including segregation of duties, awareness-raising activities, training of personnel involved in processing operations, and related audits;
- Providing recommendations on data protection impact assessment upon request and monitoring its implementation in accordance with Article 35;
- Cooperates with the supervisory authority (president of the Office for Personal Data Protection);
- serve as a point of contact for the supervisory authority on issues related to processing, including consultations conducted by ADO
- Overseeing who has access to personal data (both within the ADO organization and by external entities);
- Specifies the security measures necessary to ensure compliance with data protection regulations;
- Defines requirements related to data exchange with external entities;
- Conducts periodic security status audits (both within the ADO organization and against external entities);

Principles of personal data processing in LP

Personal data (**PII data**) - any information about an identified or identifiable natural person: (name, address, phone number, email address, date of birth, education, earnings, etc.).

In addition, from a security standpoint, sensitive data also includes PAYBACK card number information and transaction data, which when combined with personal data also gains the status of personal data.

Special categories of personal data - data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sexuality or sexual orientation of that person.

As a rule, LP does not process (collect, analyze, use for marketing purposes) special categories of personal data.

Access to personal data:

- Only those individuals should have access to personal data, and only to the extent that it is necessary for them to perform their official duties.
- Authorization to process personal data is granted by a representative of the HR Department (on behalf of ADO).
- The authorized person has no right to grant further authorizations.
- The authorization specifies the scope of data to which the employee has access.
- An authorization to process personal data shall expire upon termination of the contract entered into by the ADO with the person to whom it was granted or, if granted for a fixed period, upon expiration of the period for which it was granted.
- Anyone who processes personal data is obliged to keep confidential the information to which he has access.
- When processing data, special care must be taken and all possible measures taken to secure and protect the data from unauthorized access, modification, destruction or disclosure.

Principles of processing of personal data by external entities

If the processing is to be carried out on behalf of the ADO by external entities, the ADO shall use only such entities that provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the GDPR and protects the rights of data subjects.

Any transfer of PAYBACK participant data to an external entity (including collection of such data on behalf of LP, access to data within LP infrastructure, use of data to provide services to LP) must be approved by the DPO. Such acceptance is preceded by a security audit. For this purpose, the external entity must complete a security questionnaire provided by the DPO. In the case of entities with access to a large volume / scope of data, the DPO may decide to conduct a detailed audit at the site of such entity's operations / data processing.

The basis for transferring data to externalentities (non-controllers of such data) is a contract for entrustment of personal data processing, in which it is clearly specified:

- The purpose of the data transfer (e.g., for the performance of a given contract, for a marketing campaign),
- the activities that will be performed with the data (e.g., entry into the system, selection, segmentation of the data, conducting mailings),
- categories of data subjects (PAYBACK members, LP employees, contractors).
- The scope of the transferred data (e.g. name, surname, PAYBACK card number, telephone number),
- the period for which the entity will process the data
- method of data exchange,
- principles of further entrustment of data by a third party,
- specific responsibilities of the third party
- Consequences arising from disclosure of data to unauthorized persons (e.g., contractual penalty)

In addition, for any external entity processing such data, it is required to specify the processing location (the physical address where the servers are located, which may be different from the address of the company's office location).

Any process of acquiring personal data from PAYBACK Members or others on behalf of LP by external entities should also receive approval from the DPA. Note that in addition to the need to legally regulate such activity, there is also the need to verify that the implemented solution meets technical security requirements.

If you have any doubts about planned data processing activities, ask the DPO to resolve the doubts. Prior to the DPO's response, all activities on personal data about which there is doubt as to whether they comply with legal and technical requirements should be stopped.

General conditions for the use of computer equipment and IT security regulations

Safety measures used during work

- The presence of third parties in the area where data is processed is permitted with the permission of the ADO or in the presence of an authorized person.
- The data processor, when finished with his work, organizes his position properly securing access to documents and data media.
- Destruction of documents containing data is carried out only with a shredder or through a document destruction company. Any document containing data and not useful shall be destroyed immediately.
- When using multifunctional devices (printers, photocopiers, etc.), be very careful. Copied or scanned documents are removed from the MFP immediately after use.

Password policy

- Each user of the information system has a unique ID and a password established by him/her to authorize his/her person in the information system.
- User passwords or other credentials are subject to special protection.
- The user is fully responsible for creating a password (except for the first system password assigned by Office IT/Helpdesk) and storing it.
- Each user with access to the information systems of LP is obliged to:
  - keep confidential all their passwords or other credentials used to work on the computer system;
  - cyclically change passwords at specified intervals;
  - promptly change passwords in cases of suspected or actual disclosure;
  - Immediately change the temporary password provided by the Office IT/Helpdesk;
  - inform the Office IT/Helpdesk and the DPO of suspected or actual password disclosure;
- Passwords retain their confidentiality even after they are no longer useful.
- Prohibited:
  - writing passwords in public and placing them in places accessible to others;
  - Use of passwords based on associations, easy to guess or infer
    From information about the person, e.g. names, phone numbers, dates of birth, etc..;
  - Use of passwords that have parts of login, company name or its abbreviations in their structure (e.g. Payback123, Payback2016, etc.).
  - Using the same passwords in different operating systems and applications;
  - Sharing passwords with other users.

Rules for using the public network (Internet)

- User activities on the network for security reasons are recorded.
- Remote use of LP information systems via the public network is possible only after using a user authentication system and an encrypted transmission channel (VPN).
- For security reasons, data exchange protocols (FTP) have been disabled.
- Prohibited:

- viewing, storing and sharing content considered pornographic, racist, violent, criminal, as well as to protocols that allow file sharing on networks in violation of the law;
- Visiting websites with suspicious/doubtful reputations due to the significant risk of virus infection;
- Independent downloading and installation of software. Any such need should be consulted with Office IT/Helpdesk.

- The use of public cloud services is allowed only upon approval of the Office IT/Helpdesk.

Rules for the use of business e-mail

- The user is given a dedicated e-mail box address operating in the LP domain.
- The e-mail box address assigned to the user is used only for business or contractual purposes. Correspondence carried out electronically using LP information systems is subject to recording and may be monitored. Information sent over the LP network (including to and from the Internet) is not the private property of the user.
- Prohibited:
  - Use of the e-mail system for private purposes;
  - Sending business materials to private accounts (e.g., to work on documents at home);
  - Using the e-mail system for activities that could harm the LP's image;
  - Receiving shipments from unknown sources;
  - opening attachments with self-extracting or executable files like exe, com, etc.;
  - E-mailing executable files like bat, com, exe, multimedia files;
  - Hiding or making changes to the identity of the sender;
  - Reading, deleting, copying or changing the contents of another user's mailboxes;
  - Responding to unsolicited advertising messages and other forms of data exchange referred to as spam; if you receive such a message, please forward it to the Office IT/Helpdesk;
  - Using a business e-mail address to register on commercial, news or discussion forums that do not relate to the scope of work or contractual obligations;
  - using e-mail to advertise private goods or services, commercial and service activities other than those arising from the needs of the LP or to seek additional employment.

Rules for handling computer equipment

- Computer hardware includes, but is not limited to:
  - computers (desktop and laptop);
  - cell phones;
  - electronic media;
  - VPN keys;
  - accessories supplied together with the above-mentioned equipment or purchased separately, in particular: power supplies, bags, keyboards, computer mice, etc.
- Prohibited:
  - storing company data on private devices;
  - storing private data on LP network servers;
- Any changes to computer hardware software can only be made through Office IT/Helpdesk.
- Each user of computer equipment and electronic access cards is solely responsible for the equipment entrusted for use and is required to comply with the following rules:
  - It is forbidden to leave entrusted equipment unattended in public places;
  - It is forbidden to share the entrusted equipment with third parties;
  - Portable computers should be carried as carry-on luggage;
  - When performing professional activities at home, the user should take care to properly secure the entrusted equipment and access to information from unauthorized access by third parties;
  - Problems arising from malfunctioning computer hardware should be reported to Office IT/Helpdesk.
  - In the event of loss of entrusted equipment, this fact should be reported immediately to the DPO and the Incident Management Team The notification should be sent immediately to mojedane@payback.net or LPP_Incident_Management_Team@payback.net The notification should describe the nature of the incident, including the circumstances under which the incident occurred and, if possible, indicate the categories and approximate number of people whose data may be affected by such an incident. The Incident

Management Team will handle the notification by assessing the severity of the breach, implementing countermeasures and deciding whether to report the incident to the President of the Office for Personal Data Protection.

Final arrangements

The rules presented come into force **as of 26.03.2019.**

Management Board of Loyalty Partner Polska sp. z o.o.