Payconiq

Personal Data Protection Policy

Document Information

Document ID	PQI-DPP-POL-OO1
Classification	Internal Use
Registered on	10-04-2018
Last Modified on	13-02-2023
Business Owner	Data Protection Officer
Contact	privacy@payconiq.com
Version	6.0
Status	Final

Document Revision History

Date	Version	Change	Author
10-04-2018	0.1	Draft	Mustafa Kucukaytekin
15-05-2018	0.2	Updates for business departments	Bjarki Birgisson
25-05-2018	1.0	Approved	Duke Prins
30-10-2019	1.1	General updates following a review	Bjarki Birgisson
13-12-2019	2.0	Information added on the collection of consent to address a finding of the 2018 internal audit.	Bjarki Birgisson
14-10-2020	3.0	Review	Dries Lawrence
19-08-2021	3.1	Significant rewrite of several sections including expansion of description of DPO role.	Tim de Groot
20-08-2021	3.2	Review	Jacqueline Boucher
24-08-2021	3.3	Review	PRC
01-09-2021	4.0	Approval	Management Board
20-01-2022	4.1	Review	Jordan Bailey
22-02-2022	4.2	Review	PRC
02-02-2022	5.0	Approval	Management Board
13-02-2023	5.1	Review	Eric Lachaud/ Jacqueline Boucher

18-04-2023	5.2	Approved	PRC
26-04-2023	6.0	Approved	Management Board

Table of Contents

1. Overview

Payconiq strives to comply with applicable privacy laws and regulations related to personal data protection in countries where Payconiq operates. This personal data protection policy (this "Policy") sets forth the basic principles by which Payconiq processes the personal data of prospects, customers, employees, suppliers, business partners and indicates the responsibilities of its business departments and employees while processing personal data.

2. Scope

All PQI and PQS employees, contractors and subcontractors are required to follow the documented rules in this policy.

This Policy applies to Payconiq International S.A. ("PQI"), Payconiq Services B.V. ("PQS') and its directly or indirectly controlled wholly owned subsidiaries conducting business within the European Economic Area ("EEA") or processing the personal data of data subjects within EEA.

3. Governance

The PQI and PQS Management Boards approve Payconiq's general strategies on personal data protection.

The Data Protection Officer (the DPO) carrying out the duties as described below in this document.

The Support Department is responsible for facilitating data subjects' requests in connection with their personal data.

The Legal Department together with the DPO, monitors and analyses data protection laws and regulations and changes thereto and develops compliance requirements.

The Head of Security, is responsible for:

- Ensuring all systems, services and equipment used for storing data satisfy applicable security standards; and
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

The Product Owner or Project Manager is responsible that any new feature or project that is developed within Payconiq that involves the processing of personal data is reviewed by the DPO.

Senior Communication Officer, is responsible for:

- Monitoring whether promotional and/or marketing communications, such as emails and letters, comply with applicable legislation, including ePrivacy, General Data Protection Regulation ("**GDPR**") and relevant local law, with the assistance of the DPO and/or the Legal Department.
- Monitoring that the sending of promotional and/or marketing communications respects users' or merchants' opt-ins/opt-outs for receiving such communications.

- Where necessary, working with the DPO and/or Legal Department to ensure marketing initiatives comply with privacy laws and regulations.

The People Department is responsible for:

- Endeavouring to improve employees' awareness of the importance of protecting the personal data of users.
- Organizing personal data protection and awareness training for employees working with personal data of users.
- End-to-end employee personal data protection. It must ensure that employees' personal data is processed based in accordance with the employer's legitimate business purposes and necessity.

The Facility Team is responsible for establishing the personal data protection requirements that suppliers shall comply with.

4. DPO

4.1. Process of appointment

The DPO is appointed by the PQI Management Board. The DPO may be an internal Payconiq employee or an external contractor. Upon appointment the DPO shall, as soon as possible, ensure that the "Commission Nationale pour la Protection des Données (**CNPD**)" is informed of his/her appointment through the procedure as indicated on the website of the CNPD.

To be qualified to perform the role of DPO a person must have expert knowledge of data protection law and practices. The role of DPO may not be combined with the following roles: CEO, COO, CFO, Head of IT, Head of People, or the head of the marketing department.

Upon appointment, the identity of the new DPO shall be communicated by PQI to all employees of Payconiq.

4.2. Role of the DPO

The DPO shall function in the role of Data Protection Officer of PQI and PQS. In this role the DPO shall report directly to the Management Boards of PQI and PQS (*article 37.5* and *article 38.3* of GDPR). The DPO shall not receive any instructions regarding the exercise of the tasks of the DPO.

The DPO shall be involved in all issues within Payconiq which relate to the protection of personal data, which include but are not limited to personal data breaches, international transfers of personal data, data processing agreements with (sub)processors, new uses of personal data, and new collections of personal data. The duty to involve the DPO shall fall primarily on the Product Owner(s) and Project Manager(s) in charge of the relevant feature, product, project or relationship. However, all Payconiq employees shall have the duty to inform the DPO of any issues related to the protection of personal data if they have reason to believe the DPO has not been properly informed. The DPO shall be receptive to any information received in this regard.

The DPO shall inform and advice Payconiq of their obligations regarding the protection of personal data that they may have in relation to any significant and relevant issue relating to

the protection of personal data that the DPO is informed of. Where possible, such advice shall be communicated to the Payconiq Risk Committee ("**PRC**") and the PQI and PQS Management Boards prior to any decision being taken.

The DPO shall inform and raise awareness amongst the employees of PQI and PQS regarding the obligations of Payconiq to protect personal data. This shall consist of information sessions at the onboarding of new personnel, as well as regular trainings to existing employees. Specific training sessions may be provided when necessary to those persons who makes decisions that impact the protection of personal data on a frequent basis.

Any data processing agreement or other contract that significantly affects the processing of personal data shall be reviewed by the DPO prior to being signed by Payconiq.

In compliance with the GDPR Payconiq shall provide the DPO with reasonable assistance required for the exercise of his/her duties, which shall include the required trainings or resources to maintain his/her expert knowledge.

5. Responsibilities as controller

5.1. Basic Principles Regarding Personal Data Processing

Data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

5.1.1 Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

5.1.2 Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

5.1.3 Data Minimization

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Payconiq must apply anonymization or pseudonymization to personal data, if possible, to reduce the risks to the data subjects concerned.

5.1.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified in a timely manner.

5.1.5 Storage Period Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed, unless otherwise required by law or a competent regulator.

The period for which specific types of personal data may be retained can be found in the Information Asset Inventory. The retention times of legal documents, which may or may not contain personal data, can be found in the Legal Archiving and Retention Policy.

5.1.6 Integrity and confidentiality

Considering the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, Payconiq must use appropriate technical or organizational measures to process personal data in a manner that ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

5.1.7 Accountability

The data controller must be responsible for and be able to demonstrate compliance with the principles outlined above.

5.2. Building Data Protection in Business Activities

To demonstrate compliance with the principles of data protection, an organisation should build data protection into its business activities.

5.2.1 Notification to Data Subjects

(See the Fair Processing Guideline section).

5.2.2 Data Subject's Choice and Consent

(See the Fair Processing Guideline section).

5.2.3 Collection

Payconiq must strive to collect the minimum amount of personal data necessary for the respective legitimate purposes. If personal data is collected from a third party, it shall be ensured that the personal data is collected lawfully.

5.2.4 Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of personal data must be consistent with the information contained in Payconiq's Privacy Statements (the "Privacy Statements") and the Legal Archiving and Retention Policy. Payconiq must maintain the accuracy, integrity, confidentiality, and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. The respective business owner is responsible for compliance with the requirements listed in this section.

5.2.5 Disclosure to Third Parties

Whenever Payconiq uses a third-party supplier or business partner to process personal data on its behalf, the respective business owner must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks.

Payconiq must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards Payconiq or upon the instructions of Payconiq and not for any other purposes. When Payconiq processes personal data jointly with an independent third party, Payconiq must explicitly specify its respective responsibilities of itself and the third party in the relevant contract or any other legal binding document, such as a data processing agreement.

The entity receiving the personal data must comply with the principles of personal data processing set forth in Payconiq's Outsourcing Policy.

5.2.6 Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area ("**EEA**"), adequate safeguards as provided for in the GDPR, must be used, such as standard contractual clauses or binding corporate rules.

5.2.7 Rights of Access by Data Subjects

Payconiq's Support Department is in principle responsible for processing data subjects' request without undue delay and in any event within one month of receipt of a request. Payconiq must ensure to record the requests and keep a log of these.

5.2.8 Data Portability

Subject to the conditions set out in Article 20 of the GDPR, data subjects have the right to receive, upon request, a copy of the data they provided to Payconiq in a structured format and to transmit those data to another controller, for free. Payconiq's Support Department is responsible for ensuring that such requests are processed without undue delay and in any event within one month of receipt of a request. Payconiq's Support Department shall also assess whether each request adversely affects the rights and freedoms of others.

5.2.9 Right to be Forgotten

Data subjects have the right to request Payconiq to erase their personal data. Payconiq's Support Department shall be responsible for processing such requests internally, and to ensure that each request is processed without undue delay and in any event within one month of receipt of a request.

5.3. Fair Processing Guideline

5.3.1 Notices to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities, including but not limited to selling products, services, or marketing activities, Payconiq's Privacy Statements inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and Payconiq's security measures to protect personal data.

Changing, adding, or removing Payconiq's Privacy Statements shall be the responsibility of the DPO. If, in the opinion of the DPO, the change, addition or removal comprises a significant change of the approach within the Payconiq organization to the protection of personal data, such change, addition or removal shall be communicated to the PRC and approved by the PQI Management Board.

5.3.2 Obtaining Consents

When processing personal data, Payconiq relies on one of the following legal bases, depending on the processing activity and purpose; performance of a contract, consent, legitimate interests, or legal obligation. When personal data processing is based on the data subject's consent, Payconiq shall retain a record of such consent when possible. Data subjects shall have the option of withdrawing their consent at any time.

Consent is obtained in connection with newsletters/marketing communications, which are sent to users of the Payconiq app or other apps in which Payconiq is enabled, that have consented to receiving such communications. Users are offered the choice to opt-in for (consent to) receiving such communications during onboarding. They can also opt-in in the settings of the respective app, where they can withdraw their opt-in (consent) as well. With every marketing/promotional communication sent to users, an unsubscribe link is included, allowing users to withdraw their consent. Opt-ins and opt-outs are accurately recorded and stored in a 'live' consent registry, ensuring only users that have an opt-in (and have not opted out) will receive marketing communications.

To enable certain Payconiq features, users may need to consent to Payconiq accessing their location, phone contact list, camera, push notifications and photo library (for setting a profile picture), as further explained in the Payconiq consumer privacy statement. However, users consent to this via the settings of their phones, being prompted to do so in an in-app message. Therefore, such consents are not recorded in a registry. Users can withdraw their consents in the settings of their phones.

5.3.3 Data Protection Impact Assessments (DPIA)

GDPR article 35 states: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

The determination of whether a DPIA needs to be performed in any specific case shall be made by the DPO, subject to a veto by the PQI and PQS Management Boards.

5.3.4 Personal Data Breach

The process for identifying and handling personal data breaches is described in the Data Breach Procedure.

5.3.5 Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which Payconiq operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

6. Responsibilities as processor

Where Payconiq processes personal data on behalf of a controller, it acts as a processor for such controller and shall do so in accordance with the documented instructions of the controller. Such instructions shall be written down in an agreement or policy document, which shall be subject to review of the DPO. Such documents shall at least include determinations as to which subcontractors' personal data of such controller can be shared with and to which countries the personal data of such controller can be transferred. It also provides a legal basis for Payconiq to carry out processing activities on behalf of the controller.

Payconiq, acting as a processor, practises a facilitating role and shall fully adhere to instructions given by the controller. However, it shall not follow instructions of the controller which it expressly knows to be contrary to law. As a processor, Payconiq shall comply with the retention periods of personal data given by the controller (which are registered in Payconiq's internal data processing records) and shall not conform to its own retention periods. Payconiq shall maintain a record of all categories of processing activities carried out on behalf of the controller. When processing personal data, Payconiq shall commit to confidentiality about the personal data that is being processed. In the event of a data breach, Payconiq shall notify the controller as soon as possible (as instructed by the controller). Appropriate technical and organisational measures shall be taken by Payconiq to ensure secure processing of personal data that complies with the requirements of the GDPR.

7. RACI Matrix

	Mgmt. Board	DPO	Legal Dept.	Head of Security	Product Owner/project Manager	HR	Marcom/Head of Lux	PRC	Risk Dept.
Informative training sessions to employees	C/I	R	C			A			
Ensures PQ's compliancy with Personal Data Protection Principles.	A	R	C			I		C	I
Processing and replying to Data Subjects' request in relation to their Personal Data.	A	R	C						
Changing, adding, or removing Payconiq's Privacy Statements	A	R	C/I				I		
Approve Payconiq's general strategies on Personal Data Protection.	A	R						C/I	
Monitors and analyses data protection laws and regulations and changes thereto and develops compliance requirements.	C/I	R	A					I	C
Ensuring all systems, services and equipment used for storing data satisfy applicable security standards.	C/I	A		R				C/I	C
Performing regular checks and scans to ensure security hardware and software is functioning properly.	C/I	A		R					
Responsible that any new feature or project that is developed within Payconiq that involves the processing of personal data is reviewed by the DPO.	I	A		C	R			I	
Ensures official promotional	I	A	C				R		

and/or marketing communications, comply with applicable legislation.									
Responsible for establishing the personal data protection requirements that suppliers shall comply with.	C/I	A	C					I	R
DPIA	C/I	R		A				C/I	I

8. Policy Control

8.1 Control Measurement

Internal audit will verify compliance to this policy through various methods, including but not limited to, periodic system and log analysis, reports, red teaming exercises, and interviews with employees.

8.2 Exceptions

Any exception to the policy shall be approved by Payconiq International S.A.'s Management Board**.**

8.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of the employment.

9. Related Standards, Policies and Processes

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC);
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- ISO/IEC 27001 standard Information security, cybersecurity, and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection — Information security controls
- Information Asset Inventory;
- Legal Archiving and Retention Policy;
- Data Breach Procedure;
- Legal Archiving and Retention Policy; and
- Information Security Policy.