SECURITY POLICY

Document Reference | PL05_PP_V7

TABLE OF CONTENTS

1. References	General Data Protection Regulation 2016/679, of 27 April 2016 Decree-Law No. 242/2012, of 7 November Law No. 25/2008, of 5 June
2. Associated Documents	PL02 - Business Continuity Policy PC03 - Business Continuity Process PL03 - ML and TF Risk Management Policy PR02 - Suspicious or Unusual Operation Procedure
3. 3. Distribution List	All PayPay staff
4. 4. Document History	2018-06-05|Version 1 2018-08-16|Version 2 2018-10-09|Version 3 2018-10-25|Version 4 2018-10-31|Version 5 2019-01-02|Version 6 2020-06-04|Version 7
5. 5. Document Classification	D | Public

6. Revision Record

Version Number	Creation	Approval	Reason
	04-06-2020	**04-06-2020**	
	Compliance	**Management**	
	Inês Sousa	Tolentino Pereira	
7			Inclusion of information related to the Information Security Policy

7. Purpose and Scope

The purpose of this policy is to define procedures to avoid the use of PayPay for money laundering (ML) and/or terrorist financing (TF), according to the characteristics of the customer, as well as to avoid the possible illegal use of sensitive and personal data. Also, this policy represents the commitment assumed by PayPay, as an intermediary payment institution, with the current GDPR.

8. Applicability

A PayPayUE – Instituição de Pagamento, Unipessoal, Lda is a payment intermediary company that provides its customers, through an online portal, www.paypay.pt, payment references.

Currently, it offers four payment methods, namely: Multibanco (ATM), Multibanco Real Time, Visa/MasterCard Credit/Debit Card and MB WAY.

Paypay solo proporciona este servicio a empresas con un TIN portugués y que se encuentren domiciliadas en Portugal.

9. Commitment to Information Security

- Confidentiality

Guarantee that customer information, whose custody is entrusted to the PayPay electronic platform, is accessed only by those who are formally authorized for this purpose.

- Integrity

Guarantee the protection of the accuracy of the information received, processed, stored and transmitted under the responsibility of PayPay on its platform.

- Availability

Guarantee that the information managed is accessible, when necessary, to conduct a commercial activity, within the service levels formally defined and respecting the commitment to confidentiality and integrity.

- Data Privacy

Guarantee the privacy and trust of its holders and partners, promoting full protection over the privacy and security of personal data.

- Non-Repudiation

Guarantees that the author does not deny having created and signed a document.

- Authenticity

Guarantee the validity of the transmission, the message and its sender. The purpose is that the recipient can prove the origin and authorship of a certain document.

10. Implementation of the Information Security Policy

The Management Systems Coordinator is responsible for the definition and implementation of the Information Security Policy, Standards, Procedures and Guidelines.

All the staff is responsible for compliance with the established rules, as well as communicating to the Management Systems Coordinator any event or incident on Information Security that may affect the normal operation of PayPay.

10.1. Profiles and Responsibilities

The following staff profiles are aimed at such purposes:

Senior Management / Leadership – Responsible for coordinating the ACIN strategy and coordinating the heads of each department of the Group. The position of Senior Manager is held by the administrator José Luís de Sousa.
He is responsible for the delegation of activities, the acquisition of any equipment and services and the authorization of new information infrastructures.

Management Systems Coordinator – Responsible for ensuring that the necessary processes, policies and controls in the scope of SGQ, SGSI and SGS are established, implemented and met.
Informs the Leadership about the operation status and the needs for improvement of the management systems.
Promotes the dissemination and awareness of management systems at the level of all company units.

Internal Auditor – Responsible for participating in the performance of Audits in Management Systems and Processes, with a view to verifying and evaluating their effectiveness and compliance.
Prepares the Internal Audit plan, the Audit report, and presents suggestions for improvement.

Project coordinator – Responsible for coordinating all software development projects, and for the appointment and coordination of the Development Team.
Also, is responsible for project risk and feasibility analysis, monitoring of requirements analysis processes and solution modeling, analysis and validation of all modeling / architecture documentation created.

Programmers/Analysts – Responsible for participating in all phases of the software development and maintenance process, including requirements analysis, solution modeling and architecture, solution implementation, testing and validation of requirements, creation of manuals and supporting documentation and training of users, where appropriate.

Software Beta Tester – Responsible for conducting tests, and for testing and validating requirements.

Service Quality Analyst – Responsible for conducting tests and validation of the established requirements, creating and reviewing the content presented, and conducting internal audits of the Project Coordination Office regarding good practices for safe development.

Security Administrator – Responsible, in general terms, for implementing security policies and practices.

Systems Administrator – Authorized to install, configure and maintain systems.

Systems Operator - Responsible for the daily operation of the system from the point of view of the application. Responsible for operating the servers that support the application system daily.

Systems Auditor – Authorized to monitor system activity files and event logs for auditing.

Support Technicians – Provide technical support and monitoring to the platform.
Support Technicians are responsible for complying with the processes and policies within the Management Systems context.

Accounting Technician – Responsible for invoicing and control of ACIN accounting documents.

Administrative Technician – Responsible for the execution of various administrative tasks, necessary for the proper functioning of ACIN.

Risk Manager – Responsible for risk identification, evaluation and treatment.

Capability Manager – Responsible for ensuring the permanent availability of all the resources required to maintain continuity of operations.

Information Security Incident Manager – Responsible for ensuring a consistent and effective approach to managing information security incidents, including reporting incidents and security weaknesses.

Encryption Manager - Responsible for developing and implementing the Policy on the use of encryption controls.

Network and Communications Manage - Responsible for the management and control of communications networks for the protection of information.

IT Systems Manager - Responsible for the management and control of computer systems.

Supplier Manager – Responsible for managing the relationship with suppliers.
The Supplier Manager is responsible for compliance with the processes and policies under the SGSI.

Business Continuity Manager – Responsible for ensuring the continuous operation of the company and the timely recovery of its activity.

App Platforms Compliance Manager – Responsible for coordinating all software development projects.

Audit Manager – Responsible for participating in the Audit of the Information Security Management Systems and Processes, in order to verify and evaluate their effectiveness and compliance.

11. PayPay Security Measures

11.1 Identification of Sensitive Payment Data in PayPay

Taking into account the methods of payment by ATM (Multibanco), credit/debit cards and MBWAY, we have identified the following as sensitive payment information:

I. Customer IBAN
II. Maximum number of daily references
III. Maximum amount per reference
IV. Daily maximum amount
V. Prices

11.2 Protection of Services

PAYPAYUE uses of the 3D Secure security protocol. The 3D Secure protocol was developed by the main Credit/Debit Card brands and enables unequivocal authentication of all participants in an electronic commerce transaction. This protocol is used by VISA, under the name of Verified by Visa, and by Master Card, under the name of Secure Code. In this way, when a customer makes a payment on the www.paypay.pt portal, a process for verifying the validity of the Credit/Debit Card is activated.

The security systems linked to the 3D Secure protocol validate the identity of the customer and inform the www.paypay.pt portal about the legality of the card used for payment. Thus, it is possible to eliminate fraud and its associated costs and losses. This whole process is carried out automatically and absolutely transparent. The protection provided by this protocol, that is, in fraudulent purchases, is fully guaranteed. PayPay agrees to respond within a maximum period of two (2) business days to any request made by card users.

The www.paypay.pt portal uses the cryptographic security protocol (TSL) to safeguard the security and confidentiality of the data entered by the user (Art. 76º). It is completely safe to enter your Credit/Debit Card data in any payment made on www.paypay.pt, as all the data is entered into a Secure Server (256-bit TSL) that encrypts / encodes (that is, transforms into a code) all the confidential data related to your Credit/Debit Card.

guarantees that it does not rent or sell the data of its customers to third parties (Art. 32º), therefore all the information is confidential and used only by PayPayUE for the processing of payments and the eventual sending of communications that reinforce and personalize the cultural or product offer.

On a daily basis, PayPay promotes the continuous improvement of internal policies and procedures with a view to preventing money laundering and terrorist financing. This type of activities is materialized in compliance with applicable laws and regulations, the respect for ethical principles and by the adoption of best practices internationally adopted, as stipulated in the Law No. 25/2008, of June 5.

The company staff is obliged to strictly comply with all the duties enshrined in the current legal system, particularly with the analysis and notification of any operation that may present a ML and/or TF risk, being adequate training one of the fundamental aspects of the entire prevention system.

For the verification and confirmation of the viability and veracity of the data provided, before activating the customer accounts, a copy of the identity document of the individual customer and that of the company to which the applicant belongs is requested, in accordance with the guidelines of the Banco de Portugal (supervisory body responsible of the activities of financial institutions, according to Decree Law 242/2012).

11.3. Secure Payment Guarantee

When an IBAN needs to be changed added or deleted to receive funds, it must be done by the legal representative of the entity defined in PayPay.

In this way, only customers can request the IBAN change, excluding the possibility that a PayPay employee alters the account by mistake or even intentionally, reducing the possibility of fraud.

The request is made directly at www.paypay.com, after customer authentication. When a request for modification or addition of a new IBAN occurs, an email alert is sent to the *Compliance*. The IBAN supporting document must be sent by the legal representative of the company that made this request on the platform, in order to guarantee that:

•The legal representative indeed requested the modification of the IBAN;
•That the registered IBAN belongs to the entity.

After written confirmation, the Compliance approves the IBAN, attaching the supporting document in the client's file on the platform.

Due to the procedure implemented by PayPay, the client can only request the change, but cannot, in any way, effectively modify the IBAN directly on the platform, as this requires, necessarily, the validation of PayPay.

11.4. Control of High-Risk Customers

When PayPay receives information from the Banco de Portugal regarding a customer considered as high-risk, PayPay registers that information on the platform, so that if a customer included in this list registers, the platform issues an alert in the approval form and blocks his/her approval.

In the case of an already registered customer using PayPay, when entering the data as a High-Risk Customer, the platform issues an alert to Compliance, so that it can inform the customer and disable access to PayPay.

11.5. Monitoring and Measurement of Operations

Monitoring and measurement control operations of PayPay use the following indicators:

I. Monthly amount received greater than the customer's monthly average;
II. Monthly amount received less than the customer's monthly average;
III. Collections by reference;
IV. Number of collections per month.

11.5.1. Issuance of Notifications

The platform sends alerts to the Compliance, by email and to the TOC, in its absence, whenever there is suspicion of operations related to ML/TF, previously defined in the platform, namely:

V. Increase of more than 40% of the amounts received, in a given month;
VI. Amount received less than 40% of the monthly average;
VII. Occasional transactions for an amount equal to or greater than € 3,000.00;
VIII. VIII. Reception of 300 or more monthly payments in an entity, except when established in the customer profile.

Whenever any of the indicators mentioned above is detected, the *Compliance* of PayPay must communicate this information to the supervisory entity of Payment Institutions.

12. Risk Management

In order to guarantee the availability and compliance of the internal control system, PAYPAY undertakes to identify, analyze, qualify and address the risk derived from various sources of threats to its commitments.

The ML / TF Risk Management Policy establishes the methodology adopted to treat the identified risks, based on the best practices defined by the international reference standards, thus constituting a company management tool.

12.1. Identification of the Main Risks

Taking into account that it is a fully web platform, hosted and developed using *Cloud Computing* as an operating paradigm, a set of generic scenarios that can have an impact on the activity of PAYPAYUE has been identified, namely:

- Failure in Information Systems;
- Work Absenteeism;
- Failure in Information Security and / or Malicious Acts;
- Failure on the value chain providers;
- Failure or unavailability of the physical structure / Natural Disasters (fires, meteorological anomalies);

In the event of any of these incidents, the first objective will always be to safeguard the physical integrity of PAYPAYUE employees and quickly restore services to normal operation.

12.2. Analysis of the Impact on Operations

After the occurrence of an incident, it will be necessary to assess the damage caused by the anomalous situation. To this end, the following will be addressed:

- Cause of the anomalous situation;
- PayPay area affected;
- Status of the physical infrastructure (conditions of the electricity supply systems).;
- Conditions of operation of PayPay's technological infrastructure (Information Technology -IT- and communications equipment);
- Potential of the incident to cause additional loss or damage;
- Estimated time to recover normal operating conditions.

The situations not mentioned lack the *Compliance* analysis.

The results of the damage assessment and its impact on the company must be compared with the activation criteria of the Service Continuity Plan, which are:

Typology	Criterion Description
Building	Lack of physical access to the building or evacuation of the building
	The PayPay headquarters building does not guarantee the necessary security for its habitability
Legal	Formal regulatory investigation or inquiry
	Any incident that may affect our ability to comply with legal or regulatory obligations and / or that may affect our license as an operator.
Data Loss/Violation	Any incident that puts the brands or reputation of the company at risk as a result of serious data loss and/or unauthorized access to our networks or systems.
Level of unavailability of the service	When the extent of the damage suffered by PayPay's technological infrastructure causes an interruption in the operation of the IT or communications equipment that supports the most critical services, it is expected that this interruption will exceed the maximum time allowed for its repair.

12.3. Impact Assessment

The risks that may arise from eventual failures generally have a low probability of occurrence, but the negative impacts that may arise from them may jeopardize, in whole or in part, the operation of the company over a long period, if preventive measures are not implemented.

All risks and threats have different related resources, which promotes a differentiated evaluation according to their determined risk level. The following table presents the average of the values of each risk, taken from the Risk Analysis Matrix (DS07)

Risk Assessment Process				
Identification of Risks	Risk Analysis			Response Times
	Probability	Consequence	Risk Level	
Failure in Information Systems	C	3	III	R.T.O. < 4h
Work Absenteeism	C	1	V	R.T.O. < 4h
Failure in Information Security and / or Malicious Acts	B	3	III	R.P.O. < 24h R.T.O. < 4h
Failure on the value chain providers	B	3	III	R.T.O. < 4h
Failure or unavailability of the physical structure	B	2	III	R.P.O. < 24h R.T.O. < 4h M.A.O. < 48h
Natural Disasters (fires, meteorological anomalies)	B	4	II	R.T.O. < 4h

Risk Level

Level	Priority	Mitigation Actions
I (Very Hight)	1 (highest)	It is mandatory that the risk has already been treated or that at least one MTR is being executed.
II (High)	2	It is mandatory to plan the execution of at least one MTR before the review of the system by the management.
III (Medium)	3	Responsibility for systematic monitoring will be attributed to the risk manager, and the *Compliance* will be notified immediately of all situations that may increase the level of risk.
IV (Low)	4	The *Compliance* will send a communication to the risk managers, about its existence and about the need to monitor the risk at regular intervals.
V (Very Low)	5 (lowest)	The *Compliance* will send a communication to the risk managers on the need to check the risk status at least once a year.

12.4. Main Risks Mitigation Plan

a)Failure in Information Systems – In cases of unavailability of the service due to failures of the data center/technical infrastructure that supports the system, the company guarantees the existence of redundancy of the critical elements of the platform, including the database, power supply and communications; guarantees a backup of the database; It has a global availability of the solution of 99.8% and a specific availability during working hours, from 09:00 to 19:00, of 99.9%; guarantees the existence of an alternative center for disaster recovery, with activation, within 72 hours; and guarantees the monitoring and operation of the solution 24x7x365, with a technical intervention time in the accommodation premises of less than 2 hours.
In the event of failure or unavailability due to the commissioning of a new version, a full backup is made before the upgrade process. If any non-conformity is identified, the system is restarted using the update script. This process lasts a maximum of 60 minutes.
PAYPAYUE is hosted in the ONI Data Center, in Virtual Machines, whose servers are spread over three locations. In the event of a total Data Center disaster where the application is hosted, and the application is not available, a telephone call is made to the ONI support service. If after that telephone call it is confirmed that there was a disaster in the Data Center, the management issues an order for ONI to restore the previous day's backups to work in one of the other two Data Centers. DNS and redirections are also modified to reflect the new location.

b)Work Absenteeism - In the event of an influenza outbreak, or alike, that reduces or threatens to infect a large part of human resources, employees will be assigned remote access via VPN, and since everyone has access to the Internet, they will be able to connect to the offices of the company and continue to perform its functions. Even pre-configured VoIP phones can be assigned to continue receiving and making calls through the PayPay facilities.

c) Failure in Information Security and / or Malicious Acts - The company guarantees the quality of the information, preventing access to the information to unauthorized persons and preventing the data from being altered or deleted without permission, by creating individual accesses.

d) Failure or unavailability of the physical structure / Natural Disasters (fires, meteorological anomalies) - In the event of infrastructure failures or the occurrence of natural disasters (fires, earthquakes, floods) and the destruction of the offices, the base of

operations moves to the private address of the company management, at Rua 6 de Maio, No. 11, Ribeira Brava. This home has Internet and areas to host employees responsible for the most critical tasks to keep the company running. It is located less than a 3-minute walk from ACIN's current facilities, allowing coordination of the office's reconstruction/recovery operations.

13. Incident Management and Business Continuity Management

All events that jeopardize PayPay's information security commitments and activity will be treated as potential incidents and, as such, will be included in the PayPay's incident management process.

The respective diagnosis of the causes, consequences, control measures and mitigation of the risks that arise will be treated in accordance with best practices, with the activation of disciplinary procedures and legal actions for those matters that are classified as intent or breach of responsibilities. assumed by third parties.

The availability of the information, without neglecting responsibility for the rest of the information security commitments, will be guaranteed by implementing responses to disruptive incidents included in the scope of the PAYPAY Business Continuity Process.

14. Training and Awareness

The systematic awareness, training and education of PAYPAY employees in information security, money laundering and / or terrorist financing is a strong commitment of the company.

15. Disclosure and Publication

Disclosure of the formalization of PayPay Leadership decisions is guaranteed through the Communication Policy.

Internal publication of documents relevant to the operation of information security is considered essential so that the staff of the company feel co-responsible and comply with and apply the guidelines established in this regard.