

POLICY

Information Security Management System

PRIVACY AND PERSONAL DATA PROTECTION

Document Reference | PL22_SGSI_V8

TABLE OF CONTENTS

1. References	Page 3
2. Associated Documents	Page 3
3. Associated Records	Page 3
4. Distribution List	Page 3
5. Document History	Page 3
6. Document Classification	Page 3
7. Revision Record	Page 3
8. Policy Purpose	Page 4
9. Risks and Implications	Page 4
10. Policy Scope	Page 4
11. Data Processing Purpose	Page 4
12. Responsibilities	Page 5
13. When and how data is collected	Page 5
14. Storage Period of Personal Data	Page 6
15. Rights of Data Holders	Page 6
16. Technical and Organisational Measures	Page 6
17. Security Measures	Page 7
18. Cookies Policy	Page 8
19. Use of cookies on the opening of our Newsletters	Page 8
20. Information collected and its use in mobile applications for Android or iOS	Page 9
21. Private Policy Amendments	Page 10
22. Privacy Policy Acceptance	Page 10
23. Questions and Suggestions	Page 10
24. Data Protection Officer Contact	Page 10
25. Online Availability	Page 11

1. References	NP/ISO/IEC 27001: 2013 A.18.1.1; A.18.1.4 General Data Protection Regulation 2016/679, of 27/04/2016
2. Associated Documents	PR05 – Identification of Legal, Regulatory and Contractual Requirements Law Nº 58/2019, of 8 August – Data Protection
3. Associated Records	RG01 – Register of Documents RG06 – Table of legal and contractual requirements
4. Distribution List	Public
5. Document History	23-01-2015 Version 1 01-02-2016 Version 2 29-12-2016 Version 3 13-02-2017 Version 4 09-03-2017 Version 5 21-05-2018 Version 6 26-11-2019 Version 7 02-01-2020 Version 8
6. Document Classification	D Public

7. Revision Record:

Version Nº	Created	Approved	Reason
	02-01-2020	02-01-2020	
8	MSC	Leadership	iMED : Inclusion of permission: Access to mobile phone camera and deletion of Bluetooth permission; GTS : Inclusion of permission: Access to mobile phone camera and Internet. PayPay : Update of point 20.
	Sandra Fernández and Sofia Meneses	José Luís de Sousa	

8. Policy Purpose

The purpose of this Policy is to define how data provided by users of the platforms developed by ACIN, as well as all personal data of employees, is processed and used.

At the organisational level, this Policy represents the commitment of ACIN leadership to comply with the principles of data processing and rights of the holders, as stated in Reg. (EU) 2016/679, General Data Protection Regulation (hereinafter referred to as "GDPR"), and in Law 58/2019, of 8 August, which ensures the implementation of the above mentioned regulation in the Portuguese context.

9. Risks and Implications

The disclosure of personal information, as defined in this Policy, is punishable under Portuguese and European Legislation (GDPR and Law Nº 58/2019).

Violations of the provisions may indicate serious offenses (art. 38 of Law No. 58/2019) and very serious offenses (art. 37 of Law No. 58/2019), which, in turn, may result in penalties with fines.

10. Policy Scope

This policy applies to the processing of all personal data of natural persons, being considered as personal data the following:

- "any information, of any nature and independently of the respective support, including sound and image, related to an identified or identifiable natural person";
- "(...) information relating to an identified or identifiable natural person («data subject»), given that "(...) an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (Article 4, GDPR).

According to article 2 of the GDPR, this Policy applies "(...) to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" conducted within the Portuguese territory, as well as outside this context (Art. 2, Law Nº58/2019), either by public or private entities.

11. Data Processing Purpose

Data collected by ACIN is intended to:

- a. Registration on the platforms by completing the respective forms;
- b. Implementation of the Contract for use, including the platform use, invoicing, satisfaction questionnaires, and communication with Customers;
- c. Statistical analysis;
- d. Processing information/support requests and complaints;
- e. Marketing, through newsletters on promotional campaigns or new functionalities.

The processing of the information collected is intended to ensure the highest levels of excellence in Customer services and to continuously improve the ability to meet his/her needs.

The data collected through website forms is intended for the processing of user requests and will not be used for any other processing. If you do not allow the processing of your data, we will not be able to accept your registration.

12. Responsibilities

The Management Systems Coordinator and the Data Protection Officer (DPO) are responsible for the definition and implementation of this Policy.

The Data Protection Officer (DPO) ensures, among other aspects, compliance of data processing with the legislation in force and verification of compliance with this Data Protection Policy.

All ACIN employees are responsible for complying with the defined rules and for reporting to the Management Systems Coordinator and the DPO any irregularities or violations of this Policy and of data protection.

It is also the responsibility of the DPO to collaborate with the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados, -CNPd -*) "(...) at its request, in the pursuit of its duties.", mainly on issues related to the processing of information that the company has in its possession and that is considered sensitive.

13. When and how data is collected

ACIN collects personal data of customers through:

- a. Completion of ACIN iCloud Solutions service registration forms on the respective websites;
- b. Completion of forms/templates, regarding requests of contacts, support services, on ACIN iCloud Solutions services websites; demonstration requests;
- c. Filing a complaint via email or telephone;
- d. Communications via email, telephone or platform.

ACIN iCloud Solutions assumes that the data collected was submitted or made available by its respective holder and that its inclusion was authorised by him/her, being considered as true and accurate.

Holders of personal data shall be informed if the collection thereof constitutes a legal or a contractual obligation, or a necessary requirement to conclude a contract, as well as whether the holder is committed to provide personal data and the consequences of not providing that data.

It should also be highlighted that only data strictly necessary for the provision of the services concerned will be collected and requested according to the explicit information on the platform and the user's options.

ACIN may collect and enter personal data of Customers in automated database with the aim to conduct activities included within the scope of its collection and processing.

14. Storage Period of Personal Data

Personal data will be stored only during the period of time required for the purposes that motivated its collection or its subsequent processing, ensuring the compliance with all legal provisions applicable to archives.

15. Rights of Data Holders

In accordance with the legislation in force, data holders have the following guarantees: the right to access, update, rectification or deletion of his/her personal data, at any time, as well as the right to object the use of data for marketing purposes. To this effect, data holders must submit a request to the contacts mentioned at the websites of ACIN Group platforms. If you consider that your data is not being used in accordance with the legislation in force, you have the right to submit a complaint before the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados*, - CNPD-).

In order to exercise the above-mentioned rights, you may contact us:

By E-mail: dpo@acin.pt;

By postal service: to our headquarters, at Estrada Regional 104, nº42-A, 9350-203 Ribeira Brava, Madeira

16. Technical and Organisational Measures

ACIN adopts all technical and organisational measures required to protect the personal data entrusted to it, in accordance with Art. 35 of the Constitution of the Portuguese Republic, the General Data Protection Regulation 2016/679, of 27/04/2016 and with the implementation of this regulation in the Portuguese territory, through Law Nº 58/2019, of 8 August.

- a. By giving access to all employees and users of the platforms to personal data, in order to allow its rectification and updating, and providing information of the purpose of the data;
- b. By signing confidentiality agreements with their employees, customers and suppliers;
- c. Data holders have the right to: access their data; request the rectification of data; erasure of data; restriction of processing; data portability; object. However, these rights may be limited in accordance with Article 23 of the GDPR, in particular as regards: State security; defence; public security; inspections by supervisory authorities; protection of data subjects or others; civil proceedings;
- d. The purpose of data collection and processing is informed upon consent. Therefore, collected data is used for contractual purposes agreed with the customer, and for the delivery of newsletters or promotions exclusively about the platforms marketed by ACIN, when previously authorised by customers;
 - o ACIN iCloud Solutions regularly informs its Customers and business partners about products/services it markets, or about any other information deemed relevant through the delivery of newsletters. Newsletter can only be received by the data subject if he/she has a valid email address and if has subscribed or provided consent;

There will be no transfer of personal data collected through the newsletter service to third parties. The subscription to newsletters can be cancelled by the data holder at any time. Consent for the storage of personal data previously provided by the data

holder for the delivery of newsletter can also be revoked at any time. The corresponding address to revoke the consent or to cancel the subscription can be found in the newsletter;

- e. Users of ACIN platforms are responsible for maintaining access and codes in a personal and non-transferable manner, in order to avoid unintended access by third parties. ACIN must be immediately informed in case of any unlawful behaviour or access violation involving your Customer session;
- f. The full content of our systems is owned by ACIN, which holds the copyright and industrial property rights over the same, with the exception of contents provided by advertisers or business partners who are identified as such.

17. Security Measures

ACIN undertakes to take appropriate security measures against destruction, loss, modification, accidental or unauthorized access or diffusion, namely through:

- Periodic system security testing;
- Use of information encryption mechanisms, both in its storage and its transmission, based on secure protocols and algorithms (TLS and SHA256);
- Personal or confidential data collection forms require the use of encrypted connections;
- Adoption of physical and logical security measures that we believe are essential for the protection of personal data of our customers, at the level of the physical infrastructure provided by the *DataCenter* used to store the information managed by ACIN systems.

ACIN cannot be held liable for any wrongful act that cannot be prevented and/or foreseen.

In the event of a security failure, the ACIN leadership, together with the DPO and the Information Management Systems Coordinator, will inform the national supervisory authority (Article 51º GDPR) and will request support from this authority to minimize the damages arising from the breach.

ACIN iCloud Solutions may transmit your personal data to third parties, provided that:

- It has the unequivocal consent of users;
- As the result of the compliance with a legal obligation, or by a decision of the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados -CNPD-*), or a court order;
- It is required for the protection of vital interests of users or any other legitimate purpose provided by the legislation;
- In this case, the user will be duly informed, giving him/her the identity of the recipients and the purpose of the processing of the transferred data.

Only duly authorised users, defined in accordance with the principles of *need to know* and *least privileges*, will be able to access the resources and information available in the applications managed or developed by ACIN.

The user is only authorised to use the contents of our application solely and exclusively for the intended purposes, and it is expressly prohibited to reproduce, publish, publicly disclose, distribute or, by any means, make the contents accessible to third parties, for purposes of public communication or marketing, being further prohibited to make any alteration to the contents.

It is expressly forbidden to the user to create or introduce in our application any type of virus or programs that may damage or contaminate it, or advise third parties to do so.

ACIN ensures the deletion of data, once it is no longer required in legal, financial and accounting terms.

18. Cookies Policy

We use cookies to analyse customers behaviour, to manage the site and to collect information about users, with the aim to customise and enhance your experience with us.

A cookie is a small text file stored on your computer or mobile devices. Cookies store information that is used to help Web sites work. We can only access the cookies created by our site. You can control cookies at the browser level. Disabling cookies may prevent the use of certain functions.

We use cookies for the following purposes:

Essential cookies – they are necessary to allow the use of some important features of our website, such as login. These cookies do not collect any personal data.

Functionality cookies – they provide functions that enhance the use of our website and enable the provision of custom features. For example, they can remember your name and email in forms.

Analytical cookies – they are used to monitor the use and performance of our website and services.

Advertising cookies – they are used to provide relevant ads based on your preferences.

Session cookies - These are temporary cookies that remain in your internet browser until you leave the website. The information obtained enables to identify problems and to provide a better browser experience.

We use Google Analytics to measure the traffic on our site. *Google* has its own Privacy Policy. If you do not want your visits to websites to be detected by *Google Analytics*, go to <http://tools.google.com/dlpage/gaoptout>

19. Use of cookies on the opening of our Newsletters

For statistical purposes, our newsletters may have a single "pixel" which lets us know if they have been opened and to check clicks on links or ads in the newsletter.

The user always has the possibility to disable the delivery of the newsletter in his/her personal area or in the newsletter.

Cookies stored on your computer can be removed through your browser settings. For more information about cookies, including to know which cookies have been installed and how they can be managed and removed, visit www.allaboutcookies.org.

20. Information collected and its use in mobile applications for Android or iOS

Information is collected on or from devices where our services have been installed, according to the permissions granted. The information collected helps us to operate, provide, understand, adapt and support our services.

Some examples of the information collected are the characteristics of the operating system, battery status and device identifiers.

Access to our applications implies acceptance of information collection and use in accordance with this policy.

Permission	Description	Platform
Access phone camera	This permission may be used to take photos or read barcodes.	iGEST, iParque, iMED, GTS
Read phone status and identification	This permission may be used to access the telephone unique identifier (IMEI), which is presented in the application settings, as well as to communicate the operating system version and the percentage of the battery for assistance on the technical support provided by our services.	iGEST
Search and use account on the device	This permission may be used to send real-time messages to the users of the application. It can also be used to enable the automatic "login" whenever the application is opened.	iParque
Access the geographic location of the mobile	This permission may be used to automatically detect the Street where the driver is located in order to start the Parking easier and faster.	iParque
Bluetooth	This permission allows all Bluetooth communications, such as a connection request, accept a connection and data transfer.	iGEST
Internet	This permission allows the connection with the mobile application server.	iGEST, iParque, iMED, GTS
USB	This permission allows the connection of external peripherals.	iGEST

When the user makes a purchase on our ACIN platforms, the information that is strictly necessary for the payment is collected. This information is transmitted to our PayPay payment gateway PayPay to proceed with the collection of the payment before the bank.

Field	Mandatory
User first name;	Mandatory for card payments
User last name;	Mandatory for card payments
User email;	Mandatory for card payments
User mobile phone number;	Mandatory for MB WAY payment method
Invoicing address.	Mandatory for card payments

21. Private Policy Amendments

We reserve the right to update and amend our policy at any time, being our responsibility to inform customers of changes that alter the consent previously agreed, being at their discretion the continuity of the contract.

If substantial changes are made to this policy, customers will be notified by e-mail or through a notice in our website.

22. Privacy Policy Acceptance

The use of this system implies your consent and acceptance of the terms of our Privacy Policy. In the event of any dispute related to the terms and conditions of use, the Portuguese law will be applicable.

23. Questions and Suggestions

The collection and processing of personal data shall be carried out in accordance with the legislation applicable and in force, and in line with the guidelines of the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados*, -CNPD-).

Any issue regarding the collection and processing of data of ACIN Group Customers will be governed by the legislation in force.

To learn more about how ACIN Group platforms manage your personal data, or to clarify any question, submit a complaint or a comment about this Privacy Policy, please contact us through the contact mentioned below.

24. Data Protection Officer Contact

ACIN iCloud Solutions is the entity responsible for collecting and processing your personal data for the purposes aforementioned in this privacy policy.

Headquarters: Estrada Regional 104, nº42-A, 9350-203 Ribeira Brava,
Madeira Tel: 707 451 451
Fax: 291 957 171
Email: dpo@acin.pt

25. Online Availability

This privacy and data protection policy is available online at:
<https://www.acin.pt/politica-privacidade>