

POLICY

Information Security Management System

PRIVACY AND PROTECTION OF PERSONAL DATA

Document Reference | PL22|SGSI_V6

INDEX

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

1. References	NP/ISO/IEC 27001:2013 A.18.1.1; A.18.1.4 Reglamento General de Protección de Datos 2016/679, de 27/04/2016
2. Related Documents	PR05- Identificación de Requisitos Legales, Normativos y Contractuales
3. Associated Registers	RG01 – Registro de Documentos RG06-Tabla de requisitos legales y contractuales
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 17-05-2018 Version 6
6. Document Classification	D Public

7. Registro de la Revisión:

Version Number	Creation 21-05-2018	Approved 21-05-2018	Reason
6	Systems Management Coordinator	Leadership	Integration with RGPD

8. Policy Purpose

The objective of this policy is to define the way in which data submitted by users of platforms developed by ACIN and all personal data from employees is handled and used.

Similarly, this policy represents the commitment of the ACIN's leadership to meet the principles of data processing and the rights of users according to Regulation (EU) 2016/679, General Regulation on Data Protection (Regulamento Geral de Proteção de Dados), hereinafter referred as "RGPD", in the organizational context.

9. Risks and Implications

The disclosure of personal information, as defined in this Policy, is punishable under Portuguese and European Legislation.

Breaches to what has been legally stated and in force (RGPD), may result in "(...) fines not exceeding EUR 10 000 000 or, in the case of a company, up to 2% of its annual worldwide business revenue. corresponding to the previous financial year (...)" (Article 83 of the RGPD).

10. Policy Scope

This policy applies to all personal data, 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 related to an identified or identifiable natural person («data holder»), given that "(...) is considered as an identifiable person any natural person that can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, a location data, an identification by electronic means or by one or more specific elements of physical, physiological, genetic, mental, economic, cultural or social factors of the referred person." (Article 4, RGPD).

According to article 2 of the RGPD, this policy applies "(...) to the processing of personal data, either totally or partially, by automatic means, as well as the processing by non-automatic means of personal data contained in files or intended to be filed".

11. Purpose of data processing

The collection of data is intended to:

- Registration on the platform, through the filling of the respective forms;
- Execution of the uses on the contract, including the use of the platform, billing, customer satisfaction questionnaires, communications with customers
- Statistical analysis;
- Processing information/support requests and complaints;
- Marketing, through newsletters, promotional campaigns, or new functionalities.

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

Data collected through forms in websites are intended for the processing of users' requests. In case the processing of data is not authorized the registration won't be accepted.

12. Responsibilities

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

The Data protection officer (DPO) ensures, among other aspects, the compliance of the data treatment with the legislation in force and the verification of compliance with this Policy and the protection of data.

ACIN employees are responsible for compliance with the rules, as well as for reporting to the Management Systems Coordinator and the DPO any irregularity or violation of this policy and of data protection.

The DPO also is responsible for the cooperation with the National Commission on Data Protection (Comissão Nacional de Proteção de Dados) "(...) at its request, in pursuit of its responsibilities.", mainly on issues related to the treatment of information that the company has in its possession and that is considered as sensitive.

13. When and how data is collected

ACIN collects personal data of customers through:

- The filling of registration forms related to services provided by ACIN iCloud Solutions, in the respective websites;
- The filling of forms/matrices, contact requests, customer support services, at ACIN iCloud Solutions services' websites, requests for demonstration;
- The submission of a claim, by email or telephone;
- Communications via email, telephone or platform.

ACIN iCloud Solutions assumes that the data collected is submitted by the respective holder, or made available by the 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 subscribe a contract, as well as whether the holder is committed to provide personal data and about if there is any consequence as a result of not providing these data.

Furthermore, it must be highlighted that only data will be collected and requested when it is strictly necessary for the provision of the concerned services, in accordance with the explicit information on the platform and the user's options.

Personal data of Customers may be collected and submitted by ACIN in automated database with the aim to implement activities concerning the scope of the collection and treatment purposes.

14. Time of storage of personal data

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

15. Rights of data holders

In accordance with the legislation in force, is guaranteed to the data holder: the right to access, update, amend or delete his/her personal data, at any time, as well as the right to refuse the use of available data for marketing purposes. In this regard, the data holder must send a request using the contact details listed on the websites of the different platforms of ACIN Group. In case is considered that data is not being treated according to the legislation in force, the customer has the right to submit a complain to 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, located on Estrada Regional 104, Nº 42-A, 9350-203 Ribeira Brava, Madeira

16. Technical and Organisational Measures

ACIN adopts all technical and organizational measures required to protect personal data entrusted, in accordance with article 35 of the Constitution of Portugal and with the General Regulation on Data Protection 2016/679, dated 27/04/2016.

- By giving access to all employees and users of platforms to personal data allowing its correction and updating, and information of the purpose of the data;
- By signing confidentiality agreements with their employees, customers and suppliers;
- Data holders are entitled to: access to their data; request the rectification of the data; deletion of data; limitation of treatment; data portability; refuse. However, these rights may be limited in accordance with what is settled in article 23 of the RGPD, especially to: State security; defence; public safety; inspection by the supervisory authorities; protection of data holders or others; execution of civil lawsuits;
- The purpose of the collection and processing of data is informed in the Act of consent. In this way, the data collected is used for contractual purposes concluded with the customer, as well as newsletters delivery or promotions exclusively about the platforms marketed by ACIN, when that has been pre-authorized by the customer;
 - ACIN iCloud Solutions informs regularly its clients and business partners about products/services it markets, or about any other information considered relevant through newsletters delivery. Newsletters can only be received by the data holder when there is a valid email address and if the data holder subscribed or provided consent to the reception of newsletters.

There will be no transfer to third parties of any personal data collected from the newsletter service. The newsletter subscription can be cancelled by the data holder at any time. The consent to the storage of personal data that was previously provided to receive the newsletter, can also be revoked at any time. For the purposes of revoking the consent or to cancel the subscription, the corresponding address can be found in any newsletter.

- Users of ACIN platforms are responsible for maintaining access and codes in a way that is personal and non-transferable, in order to avoid undesired accesses made by third parties. In case of knowledge of any unlawful behaviour or violation of access that involves the customer session, this must be immediately informed to ACIN;
- 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 the content provided by advertisers or business partners who are identified as such;

17. Security measures

ACIN is committed to take appropriate security measures against loss, destruction, modification, accidental or unauthorized access or diffusion, and cannot be considered responsible for any illicit action that is not capable to prevent or predict, in particular through:

- Periodic tests of security systems, by itself or by subcontracted entities for this purpose.
- Use of encryption mechanisms of information, both in its storage or in its transmission, being based on safe algorithms and protocols (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 the personal information of our customers, at the level of physical infrastructure offered by the DataCenter used to store the information managed by the systems of ACIN.

In case of breach of security, the leadership of ACIN, in conjunction with the DPO and the Information Management System Coordinator will seek to inform the national supervisory authority (article 51 RGDP) and to request to this entity support to minimize the damage that may result of any failure.

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

- Have the unequivocal consent of users;
- As a result of the fulfilment of a legal obligation, or by a decision of the National Commission for Data Protection (Comissão Nacional de Proteção de Dados, -CNPd-) or by a court order;
- When it is necessary for the protection of vital interests of the users or any other legitimate purpose provided by the legislation;
- When this happens, the user will be duly informed, about the identity of the recipients and the purpose of the processing of the data transferred.

Only authorized users, defined on the basis of the principles 'need to know' and 'least privileges', can access resources and information provided by managed applications or developed by ACIN.

The user is only authorized to make use of the contents of our application only and exclusively for the purposes for which they are intended, being expressly forbidden to reproduce, publish or publicly disclose, distribute or otherwise, make the content accessible to third parties for purposes of marketing or public communication, and being forbidden to carry out any modification of the content.

The user is expressly forbidden to create or enter in our application any type of virus or programs that may damage or contaminate or advise third parties to do so.

ACIN ensures the removal of data, so that they no longer be needed in legal, financial and accounting terms.

18. Cookies policy

We use cookies to analyse customers behaviour, to administer the site and to gather information about users to customize and improve 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 make Web sites work. We can only access the cookies created by our site. You can control cookies at the browser level. To disable cookies, you can impede the use of certain functions.

We use cookies for the following purposes:

Required cookies- are needed to allow the use of some important features on our site, such as login. These cookies do not collect any personal information.

Functionality cookies – provide functionality that makes more convenient the use of our site and enables the provision of custom features. For example, they can remember your name and email in forms.

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

Advertising cookies - are used to provide relevant ads according to your preferences.

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

We use Google Analytics to measure 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

Our newsletters may, for statistical purposes, contain a single "pixel" that lets us know if they are opened and it verifies the clicks through links or advertisements 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 in your computer can be removed through the settings of your browser. For more information about cookies, including to know that cookies are installed and how they can be managed and disposed of, see www.allaboutcookies.org.

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

Information is collected about 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.

Attributes, such as operating system, battery status and identifiers of devices, are some examples of collected information.

The access to our applications supposes the acceptance of information collection and use in accordance with this policy.

Permission	Description	Platform
Access to the camera of the phone	This permission can be used to take picture or to read barcodes.	iGEST, iParque
Read the status or identity of the phone	This permission can be used to access the phone's unique identifier (IMEI) which is presented in the settings of the application, and also in order to communicate the operating system version and the percentage of the battery for assistance on the technical support provided by our services.	iGEST
Find and use account in the device	This permission can 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 open.	iParque
Access the geographic location of the cell phone	This permission can be used to automatically determine the street where the driver is located in order to start the Parking in a fast and simple way.	iParque
Bluetooth	This permission allows performing all Bluetooth communications, as a connection request, to accept a connection and to transfer data.	iGEST, iMED
Internet	This permission allows the connection with the server of the mobile application server.	iGEST, iParque, iMED
USB	Allows connection of external peripherals.	iGEST

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 achieved previously, being of his/her 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. Acceptance of the Privacy Policy

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 relating to the collection and processing of information of Customers of ACIN Group will be governed by the legislation in force.

To learn more about how the platforms ACIN Group manage your personal information, or in order to clarify any question, complaint or to comment about the Privacy Policy, please contact ACIN through the contacts mentioned below.

24. Contact of the responsible persons for Data Processing

ACIN iCloud Solutions is the responsible entity for collecting and processing personal data, for the purposes afore-mentioned in this privacy policy.

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