



Corporate Privacy Policy

Version: 1.0

Date: 03/11/2020

Reference: RS.CUMPL.DPD.POL.0000

PUBLIC USE



Redsys, Servicios de Procesamiento, S.L. – c/ Francisco Sancha, 12 – 28034 Madrid (Spain)

www.redsys.es

Authorisation and version control

ISSUED BY: Carla Garde (DPD - Data Protection Delegate)	VALIDATED BY: Irene García F. Audit and Corporate Risks Area (Compliance Management)	APPROVED BY: David Blasco (Manager for Corporate Services and delegated signature for General Management)
COMPANY: Redsys	COMPANY: Redsys	COMPANY: Redsys
Signature:	Signature:	Signature:
Date: 14/10/2020	Date: 27/10/2020	Date: 27/10/2020

Notes: The management of printed documentation is the responsibility of the person who printed it.

The printed versions of the safety regulations do not guarantee to be the last approved version. To consult the latest version, access the corporate database.

For the processing of the information contained in this document, the guidelines set forth in the Redsys Regulations must be followed, and in the RS.RI.SEG.NOR standard .0003 CLASSIFICATION AND INFORMATION PROCESSING STANDARD

Version	Date	Concerns	Brief description of the change
1.0	14/10/2020	All	Document creation.



CONTENTS

1. PURPOSE AND SCOPE OF APPLICATION	4
2. PRINCIPLES IN THE PROCESSING OF PERSONAL DATA	4
2.1 PRIOR CONSIDERATIONS	4
2.2 PRINCIPLE OF LAWFULNESS, FAIRNESS AND TRANSPARENCY	4
2.3 PRINCIPLE OF GUARANTEE OF RESPECT OF THE RIGHTS FOR THE INTERESTED PARTIES	5
2.4 PRINCIPLE OF LIMITATION OF THE CONSERVATION PERIOD	5
2.5 PRINCIPLE OF SECURITY AND RISK MITIGATION	5
3. CONDITIONS FOR DATA PROCESSING AND DUTY OF INFORMATION	5
4. INTERNATIONAL DATA TRANSFERS	6
5. PRIVACY FROM DESIGN BY DEFAULT	6
6. DATA PROTECTION DELEGATE	6
7. TRAINING AND AWARENESS	7
8. MONITORING, AUDITING AND CONTROL	7
9. GLOSSARY OF TERMS	7

The copyright of this document belongs to Redsys. Its reproduction, sale, or transfer to third parties is prohibited.



1. PURPOSE AND SCOPE OF APPLICATION

The Redsys Group, as a provider of technological services in which the use of personal data is especially relevant, defends that an adequate processing of personal data represents an opportunity to improve the lives of the interested parties and contributes to the development of Company.

The Redsys Group guarantees respect for the fundamental rights and freedoms of people, among which there is the fundamental right to the protection of personal data.

Through this Corporate Privacy Policy (hereinafter, the Policy), the level of compliance is set forth and standardized by the companies that make up the Redsys Group (hereinafter the Group) formed by Redsys Servicios de Procesamiento, SL, Redsys Salud, SL and Gestora Patrimonial Francisco Sancha SLU, of the most guaranteeing standards and good practices regarding the protection of personal data and privacy.

This Policy is mandatory and applicable, for which it applies to all Group companies, their employees, managers, administrators, and collaborators.

Consequently, all of them have the obligation to know, understand and comply with the guidelines contained in this policy, being these in turn those that put into practice, actively promote, and supervise the fulfilment of these principles and objectives in their different fields of activity and responsibility.

2. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

2.1 Prior considerations

In the processing of personal data conducted by the Redsys Group, either for its internal organization or to make possible the provision of technological services as a provider, they will be done in accordance with the following basic principles, set out in the reference regulations in this regard:

- Principle of lawfulness, fairness, and transparency
- Principle of guarantee of respect for the rights of the interested parties
- Principle of storage limitation
- Principle of security and risk mitigation.

2.2 Principle of lawfulness, fairness, and transparency

In accordance with article 5.1, section a) of the General Data Protection Regulation (hereinafter RGPD), the Redsys Group will adopt the necessary measures and protocols to guarantee that the personal data that it processes in any way are processed in a lawful and fair manner.



All parties bound by this policy must ensure that personal data used in any processing, both as data controllers and processors, will always be collected for legitimate purposes and will not be processed in any way incompatible with those purposes.

In relation to compliance with the duty of transparency with the interested parties, the Group and its employees, managers and collaborators guarantee that they will always provide accessible and easily intelligible information on aspects such as the type of data we collect, the channel or method of collection and processing, their purpose or the period for which we keep them, as well as whether we transfer or communicate personal data to third parties.

2.3 Principle of guarantee of respect for the rights of the interested parties

The Redsys Group makes clear and simple tools and procedures available to interested parties to ensure that they can always exercise their rights in accordance with current legislation on data protection.

The different departments and / or areas, as well as the Data Protection Delegate him/herself that are likely to exercise before them any of the rights in terms of data protection, guarantee to comply with the terms and forms described in the current legislation when responding to them.

2.4 Principle of limitation of the conservation period

The Redsys Group will not keep the personal data it processes from the different data subjects with whom it interacts for longer than the time required to comply with the purposes defined and the current legislation on data protection or the specific legislation that applies or may apply to each specific processing.

2.5 Principle of security and risk mitigation

In compliance with article 32 of the GDPR, the Redsys Group will process the personal data of interested parties by applying the necessary and appropriate technical and organisational measures and controls to guarantee the confidentiality, integrity, and availability of the information, ensuring a level of security appropriate to the level of risk of the specific and individually assessed processing.

3. CONDITIONS FOR DATA PROCESSING AND DUTY OF INFORMATION

The Redsys Group will process the personal data of the interested parties in accordance with the bases of legitimacy set forth and described in the current legislation on data protection, specifically in article 6 of the RGPD.

At all times in which personal data are collected, clear, concise, and transparent information will be offered about the processing of the data, such as the identity of the controller for the processing and



the contact details of the DPO, the purpose for which they will be used, the basis of legitimacy according to which they are collected, if they are transferred or communicated to third parties or if they are the subject of an international data transfer.

As a rule, this information will be offered in a layer system, a first layer of basic information that will refer to a second layer of additional and detailed information, in accordance with the recommendations in this regard issued by the competent authority in Spain, the AEPD.

In any case, all the subjects bound by this policy confirm that no personal data will be collected or processed without an appropriate legitimation basis and verified by the company's DPD, as well as without having offered basic privacy information based on Articles 13 and 14 of the RGPD prior to processing.

4. INTERNATIONAL DATA TRANSFERS

As a rule, the Redsys Group in its normal data processing operations does not transfer personal data to countries outside the European Union that do not have an adequacy decision.

However, on those exceptional circumstances in which international transfers are made, they will be made based on the cases described in articles 45 to 49 of the RGPD, and they will be conveniently informed in the privacy policies in which it applies in accordance with the guidelines of the duty to inform.

5. PRIVACY FROM THE DESIGN BY DEFAULT

In application of article 25 of the GDPR, the Redsys Group has established protocols and mechanisms that guarantee that any new project or task initiated in the company has an *ad hoc* privacy analysis that guarantees compliance with principles such as minimisation or the need-to-know principle, preventing more data from being processed than necessary or by more people than is due for the fulfilment of the intended purpose.

6. DATA PROTECTION DELEGATE

To guarantee the data protection rights of all those interested parties with which the Redsys Group is related, adequate resources have been allocated for the implementation of this Policy, as well as the applicable regulations on data protection.

One of the essential roles for this is the Data Protection Delegate, who is the Group's corporate representative for the protection of personal data. The main functions of the Group DPD are:

- Supervision of compliance with current regulations on data protection.



- Consultancy on data protection matters to all the company's units that require it, both business and corporate.
- Implementation and application of privacy and data protection policies, and assessment of the impact on the matter of new projects that process or contain personal data.
- Communication with the competent control authorities and interested parties in the context of their area of responsibility.
- Compliance with all those powers and functions assigned by the reference regulations, among others, those contained in article 39 of the RGPD.

7. TRAINING AND AWARENESS

The Redsys Group is committed to the firm conviction that the effective application and implementation of the rights and obligations enacted by the data protection regulations requires the undeniable establishment of a culture of knowledge and compliance with these regulations by every one of its employees.

In this regard, the Group, on an annual basis and since the entry into force of the GDPR, has provided training on the subject using the teaching platforms available to the company and adapting said training to the extent possible to the relationship of each employee with the data, in accordance with their work competences.

8. MONITORING, AUDITING AND CONTROL

The Redsys Group, in its commitment to supervision and continuous improvement, periodically submits its processing of personal data to internal or external controls and/or audits in order to verify correct compliance with the regulations in force on the matter applicable to each processing, with this Policy, as well as with the different rules and procedures that develop it, recommending in each case the relevant corrective or improvement measures.

Additionally, and in application of article 42 of the RGPD, the Redsys Group is working to implement and certify in the context of its Integrated Management System (hereinafter SGI) the ISO 27701 standard, specific to privacy.

9. GLOSSARY OF TERMS

- **Personal data:** all information about an identified or identifiable natural person (the "**Interested Party**"). An identifiable natural person is any person whose identity can be established, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location



data, an online identifier or one or more elements of the physical, physiological, genetic, mental, economic, cultural, or social identity of said person.

- **Processing:** any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated or non-automated procedures, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- **Data controller:** the natural or legal person, public authority, service, or other body which, alone or jointly with others, determines the purposes and means of the processing.

- **Data processor:** the natural or legal person, public authority, service, or other body which processes personal data on behalf of the data controller.

- **Recipient:** a natural or legal person, public authority, agency, or another body, to which the Personal Data are disclosed, whether a third party or not.

- **Third party:** a natural or legal person, public authority, service, or body other than the person concerned, the controller for the processing, the processor and the persons authorised to process personal data under the direct authority of the controller or the processor.

- **DPD:** person in charge for ensuring compliance with the regulations on data protection within the company in accordance with Section 4 (arts. 37 to 39) of the RGPD as well as the sixth section of this Policy.

- **Personal data security incident:** any information security incident that causes the destruction, loss or accidental or illegal alteration of personal data transmitted, stored, or otherwise processed, or the unauthorized communication or access to said data.

- **Special categories of data:** These are personal data that can only be processed when certain requirements imposed by the applicable regulations are met, as well as those that, due to their special nature, the Company considers at any time. They are as follows:

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.
- Genetic data.
- Biometric data.
- Health data.
- Data concerning a natural person's sex life or sexual orientation; and
- Data of a criminal nature.

