CORPORATE DATA PROTECTION POLICY ROVI GROUP

July 2024

Contents

1. INTRODUCTION

This Corporate Personal Data Protection Policy (hereinafter, the **"Policy"**) is intended to ensure that all personal data processing activities carried out by the companies that form the **ROVI Group** (hereinafter, **"ROVI"** or the **"Group"**, without distinction) comply with the principles, requirements and obligations of the General Data Protection Regulation (hereinafter **"GDPR"**) and the data protection laws in force in the territories where the Group operates (for example, Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights), as well as any other legal texts with privacy and data protection implications (as a whole, the **"Applicable Regulations"**)

Thus, the goal of this Policy is to inform all those persons who take part in or are responsible for personal data processing activities in the Group of the fundamental bases and essential criteria for internal action, in order to ensure that the personal data processing within their sphere of responsibility is conducted respecting the governing principles of data protection and meeting the obligations established in the regulations.

This Policy will be revised and updated in the light of any changes in the law, case law or doctrine that arise in relation to the Applicable Regulations, as well as any organisational or technological changes that may take place in the ROVI Group, and will always be available for consultation on the ROVI Group's corporate website.

2. SCOPE OF APPLICATION

This Policy is mandatory and applies to all ROVI Group companies in relation to any personal data processing that takes place within their business operating processes. In particular, it will be applicable to all internal and external personnel, suppliers and anyone who processes personal data on behalf of ROVI in the course of their activity.

The Policy does not, and does not seek to regulate the internal application of the obligations of the Applicable Regulations exhaustively. In this respect, the specific processes, responsibilities and tasks of the compliance areas will be expanded and specified in implementing documents (for example, internal instructions, policies, procedures or SOPs). This Policy and its implementing documents constitute the rules of the ROVI Group's privacy and data protection management system.

3. DEFINITIONS

The following definitions are provided to facilitate a common understanding in ROVI of the relevant personal data protection concepts included in this document.

- **Supervisory authority**: independent public authority established by a Member State of the European Union responsible for supervising any aspect related to privacy and personal data protection.

- **Personal data:** any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as, for example, 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.

- **DPO or Data Protection Officer:** person responsible for the supervision of compliance with data protection obligations in the ROVI Group who acts independently. His or her functions are established in the GDPR and, additionally, in this Policy.

- **Data subject:** natural person to whom the personal data relate (for example, ROVI Group employees, persons reporting adverse effects, healthcare professionals, patients participating in trials promoted by ROVI, even when their data are pseudonymised, etc.).

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

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

- **GDPR:** General Data Processing Regulation

- **Personal data processing**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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.

4. PRINCIPLES CONCERNING PERSONAL DATA PROCESSING

The Applicable Regulations set out a series of principles that must be respected when configuring and developing any personal data processing that is carried out by Group companies. These principles are mandatory for all persons providing their services in the ROVI Group.

However, the Regulatory Compliance Department may specify how to comply with these principles by drawing up internal procedures, which will also be mandatory.

Each department of ROVI that processes personal data must work proactively to comply with the principles listed below. To this end, they may request the assistance of the Regulatory Compliance Department.

4.1. Principles of lawfulness, fairness and transparency

The personal data of the data subjects will be processed **lawfully, fairly and in a transparent manner** in relation to the data subject.

For the processing to comply with this principle and be **lawful**, it must be based on one the legitimate bases set out in the GDPR. In particular, the cases in which personal data processing may be carried out legally are the following:

- Consent of the data subject;

- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- The existence of a legitimate interest pursued by the controller or a third party;
- The need to comply with a legal obligation to which the controller is subject;
- The need for the controller to take steps in relation to a contract;
- The need to perform a contract to which the data subject is party; and
- The need to protect the vital interests of the data subject or another natural person.

Likewise, for the data processing to be **transparent and fair**, data subjects must be informed of the processing activities that the Group carries out with their personal data in an information clause. This information must be provided to data subjects both when the personal data have been obtained from the data subject and when they have been obtained from third parties.

4.2. Purpose limitation

When personal data are obtained, they must be collected for **specific, explicit and legitimate purposes** and may not be further processed in a manner that is incompatible with the purposes for which they were initially collected.

According to this principle, the purpose of the processing must be clearly defined before the personal data are collected and, in any case, the processing must not infringe the law.

4.3. Data minimisation principle

The personal data collected for processing must be **adequate, relevant and limited** to what is strictly necessary in relation to the purposes of the processing for which they have been collected. Therefore, no personal data may be collected other than those strictly necessary to complete the purpose for which they were collected.

4.4. Accuracy principle

The personal data must be **accurate** and **kept up to date**.

In this respect, ROVI must ensure that all the information repositories, including applications, platforms, websites, databases, etc., contain accurate and complete information.

To comply with the principle of accuracy, the departments that process personal data must establish **regular review processes** for the information, in order to check that the personal data stored in the ROVI systems for which they are responsible are accurate and up to date.

4.5. Data storage limitation

Personal data may not be stored for longer than necessary to complete the purposes for which they were collected.

When the purpose for which they were collected has been completed, personal data may only be stored if they are blocked under security measures that guarantee that they cannot be accessed, viewed or, in short, processed for any purpose other than making the data available to judges and courts, the prosecution service or the competent public authorities in relation to claims for any possible liability derived from the process during the period covered by the statute of limitations.

Once the statute of limitations for any claims that might be filed for possible liability derived from the processing, the personal data must be destroyed.

4.6. Principle of integrity and confidentiality

The personal data of data subjects must be processed in a manner that ensures their security, applying technical and organisational measures appropriate to ensure a level of security appropriate to the risk and prevents the unauthorised or unlawful processing or accidental loss, destruction or damage.

4.7. Accountability principle

The ROVI Group will be responsible for compliance with the provisions of the data protection regulations and must be able to demonstrate said compliance to the data subjects and relevant Supervisory Authorities.

Therefore, it is particularly important that all the technical and organisational measures that are implemented in order to comply with the requirements of the GDPR and the Applicable Regulations are properly documented in order to be able to demonstrate due compliance.

5. LEGAL OBLIGATIONS IN RELATION TO PERSONAL DATA PROCESSING

The Applicable Regulations set out a series of obligations that all ROVI companies must meet when they process personal data in the capacity of data controller, as set out below.

5.1. Duty to inform

In cases where ROVI acts as data controller, the data subjects must be informed of the processing activities to be performed on their personal data.

To comply with the foregoing, either when the data are collected (if they are obtained directly from the data subject) or at the time of the first communication with the data subject (if they are not obtained directly from the data subject), the department responsible for the personal data must request the Regulatory Compliance Department to provide an information clause adapted to each processing activity.

5.2. Privacy by design and by default

The ROVI Group must ensure that, both in the initial design phase of any project or initiative that entails new personal data processing and during the data processing itself, appropriate technical and organisational measures are implemented.

To this end, the persons who provide their services to ROVI must involve the Regulatory Compliance Department as from the initial phase of the project/initiative that entails personal data processing, in order to assess, inter alia, the risks to which the personal data could be exposed, taking account of the context and the diverse factors that influence ROVI's business processes.

5.3. Records of processing activities

Each ROVI company has a Record of Processing Activities (**"RoPA"**) that sets out details of the personal data processing carried out by each Group company in the capacity of either data controller or data processor and contains the information required by the GDPR.

The RoPA of each of the companies will be reviewed periodically, and whenever there is a significant change in any of the processing activities, to ensure that the information is accurate and up to date.

The persons who provide services in the ROVI Group are obliged to notify any new personal data processing beforehand and to report any substantial change in the nature of the processing carried out in the area of their functions.

5.4. Risk management of the rights and freedoms of data subjects

The data protection regulations establish ROVI's obligation to conduct an objective assessment of the risks inherent to each one of the processing activities recorded in the RoPA and prior to recording a new processing activity, in order to establish whether the data processing involves a high risk for the rights and freedoms of natural persons.

If it is likely that the data processing involves a high risk for the rights and freedoms of natural persons, ROVI will conduct the relevant Privacy Impact Assessment (hereinafter, **"PIA"**).

5.5. Relations with third parties

In many cases, signature of any type of contract, agreement or proposal with third parties will involve access to personal data for which ROVI is the controller or an exchange of personal data. For example, data of employees, healthcare professionals, analysts and investors, website users and any other personal data that are managed in the course of ROVI's activity.

Therefore, **before entering into any type of agreement, contract or proposal that entails personal data processing, it will be necessary to consult the Regulatory Compliance Department.**

In the analysis of its relations with third parties, in particular when a data processor is necessary, ROVI must ensure that said processor provides sufficient guarantees that it will apply appropriate technical and organisational means in the personal data processing. There is, therefore, a **duty of diligence when choosing the external supplier** that will act as processor and, in order to comply with this obligation, it is essential that the Regulatory Compliance Department be informed, with due notice, of any contract that entails the processing of personal data.

5.6. Personal data breaches

A personal data breach is a security incident that affects personal data. Depending on the circumstances, a breach may affect the confidentiality, availability and/or integrity of the personal data at the same time or any combination of them.

All the persons who form part of the ROVI Group are under the obligation to report, as soon as possible, any incident of which they are aware that takes place in the information systems that contain personal data, irrespective of the media that contains them (for example, information systems, paper documents, USB flash drives, etc.), even if the evidence is circumstantial.

5.7. Rights of data subjects

Data processing regulations confer on the data subjects rights that they can exercise in respect of ROVI in order to know and control the processing that the Group carries out in relation to their personal data, specifically:

- **Right of access:** enables the data subject to contact ROVI to find out whether or not personal data concerning him or her are being processed and, where this is the case, obtain information on the subject and a copy of the data.

- **Right to rectification:** enables the data subject to request the rectification of inaccurate personal data concerning him or her. Likewise, the data subject will have the right to have incomplete personal data processed by ROVI completed.

- **Right to erasure or "right to be forgotten":** the data subject will have the right to the erasure of his or her personal data when a series of circumstances exist.

- **Right to restriction of processing:** the data subject will have the right to request restriction of processing of his or her personal data when a series of circumstances exists.

- **Right to data portability:** the data subject will have the right to receive the personal data concerning him or her, which he or she has provided to ROVI, and to transmit them to another controller without hindrance from ROVI, provided the processing is based on the consent of the data subject and uses automated means.

- **Right to object**: allows the data subject to object to ROVI's processing his or her personal data for a specific purpose when a series of circumstances exists.

- **Right not to be subject to individual automated decision-making:** this right is intended to ensure that the data subject is not subject to a decision based solely on automated processing of his or her personal data, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The information clauses that are provided to data subjects must include information on the possibility of exercising these rights, including the mechanisms, allowing the data subjects to exercise these rights free of charge.

The data subject may exercise his or her rights in respect of ROVI when the latter is the data controller at the email address protecciondedatos@rovi.es or by ordinary post, telephone/website, etc.

Personnel who, in the course of their functions, note that one of these rights is being exercised outside the channel enabled for this purpose, or as soon as a request to exercise a right is received must notify the Regulatory Compliance Department as soon as possible, within a maximum period of twenty-four (24) hours, by sending an email to protecciondedatos@rovi.es. Personnel receiving such requests may not reply directly to the exercise of a right by a data subject.

5.8. Training and awareness

All ROVI employees who, in the course of their professional duties, have access to personal data must periodically take a data protection training course and pass the relevant evaluation test. This annual training is intended to inform employees of the GDPR-derived obligations to which ROVI is subject.

Furthermore, employees from specific departments may be required to carry out additional data processing training activities as may be defined by ROVI.

6. ROLES AND RESPONSIBILITIES OF THE PRIVACY FUNCTION IN THE GOVERNANCE MODEL

For the management, operation, oversight and compliance of the data protection management system, the ROVI Group has defined the following roles and responsibilities:

- **Audit Commission**: internal body of the Board of Directors that holds, among others, the responsibility of regularly reviewing and overseeing the internal control and risk management systems of the ROVI Group, as well as their efficacy in appropriately identifying, managing and making known the main risks. As part of these responsibilities, the Audit Commission is responsible for managing data protection risks.

- **Compliance Committee:** body that advises the Audit Commission of the ROVI Group on regulatory compliance.

- **Regulatory Compliance Department:** area that performs the day-to-day activities in coordinating regulatory compliance in the ROVI Group from a global perspective in order to ensure the company's compliance. Likewise, it is in direct communication with the Compliance Committee to report the ROVI Group's compliance status and provide advice when necessary.

- **DPO of the ROVI Group:** the global DPO is responsible for overseeing compliance with obligations in the ROVI Group and the management of the management system, as well as coordinating and ensuring compliance with the guidelines issued to the entire organisation, in coordination with the ROVI Group's Regulatory Compliance Area.

- **Privacy Champion:** a Privacy Champion has been appointed at each subsidiary to provide local support to the global DPO in implementing policies, guidelines and organisational measures in the companies that form the ROVI Group. The Privacy Champion is the main local contact to centralise any issues that may arise in relation to privacy and, where applicable, will liaise with stakeholders at local level.

7. ACCOUNTABILITY

To find out whether the measures and procedures implemented by the ROVI Group are appropriate and are working correctly and as expected, the ROVI Group DPO will, with adequate frequency, collect the necessary evidence and evaluate the level of internal compliance on the part of the ROVI Group entities (or some of them).

The frequency and the selection of the specific controls will be determined internally by the ROVI Group DPO for each review process. The relevant areas in which the controls are conducted will at all times collaborate in obtaining and managing the evidence that is necessary to perform the evaluation.

The results of the review process will be documented appropriately and, if applicable, will be included in a report.

At least once a year, the DPO will prepare a document that sets out the main regulatory compliance milestones in relation to data protection in the ROVI Group over the last year. This document will include at least an explanation of the main compliance risks detected, metrics in relation to the exercise of rights and security incidents, the evolution of the management system and the results of the compliance controls implemented.

The compliance report will be escalated to the senior management of the ROVI Group for any issues derived from the information reported. Prior to escalation, the content of the report will be reviewed by the Compliance Committee.

8. DUTIES AS AN EMPLOYEE

To ensure compliance with all the principles and obligations set out in this Policy in accordance with the Applicable Regulations, all ROVI Group employees undertake to comply with the following rules:

1. To notify the Regulatory Compliance Department prior to any new personal data processing and of any substantial change in the nature of the data processing carried out in his or her functional area.

2. To process the personal data that he or she accesses solely to comply with his or her functions, respecting the principles of lawfulness, fairness, transparency, limitation, minimisation, accuracy and confidentiality.

3. To ensure that his or her functional area has **processes for regular review** of the information to verify that the personal data stored in ROVI's systems for which he or she is responsible are accurate and up to date.

4. Not to use the personal data that he or she accesses to perform his or her duties for any purpose other than that or those for which they were collected.

5. Not to disclose to, send to or share with third parties outside the ROVI Group any of the company's information that contains personal data to which he or she has had access in the course of his or her functions. Sending personal data outside ROVI must be previously consulted with the Regulatory Compliance Department.

6. Not to share personal data with other business areas in the company, except in cases authorised by the Regulatory Compliance Department.

7. To involve the Regulatory Compliance Department as from the initial phase of any project/initiative that entails personal data processing.

8. To define, jointly with the Regulatory Compliance Department, an information clause adapted to each processing activity to be provided at the time the data are collected and in the first communication with the data subject.

9. To consult the Regulatory Compliance Department before signing any type of agreement, contract or proposal that entails personal data processing.

10. Each department is responsible for defining, jointly with the Regulatory Compliance Department, the periods for storing and blocking the personal data it processes. All ROVI Group employees must respect the storage and blocking periods defined and ensure that personal data are not stored indefinitely. If an employee is aware that the storage period for personal data has been exceeded, he or she must inform the Compliance Department immediately.

11. To notify the Regulatory Compliance Department and the Head of Security, as soon as possible, of any incident of which he or she is aware that may occur in the information systems that contain personal data, regardless of the media on which the information is stored (for example, information systems, paper documents, USB flash drives, etc.), even if the evidence is circumstantial.

12. To notify the Regulatory Compliance Department of any request to exercise a right that is received through any of the channels enabled for this purpose within a maximum period of twenty-four (24) hours.

13. To read and comply with the Corporate Data Protection Policy, which sets out in full the data protection obligations and principles that must be applied when personal data are obtained, accessed and/or used. Remember that failure to comply may be a disciplinary infringement.

14. **When in doubt, always consult the Regulatory Compliance Department.**