DATA PROTECTION POLICY

Version:	Made by:	Reviewed by:	Approved by:	Date:	Status:
1	CCO	General Counsel	Compliance Unit	17/09/2020	Active

SGRP-Policy-Data Protection Policy

ITÍNERE GROUP CORPORATE DATA PROTECTION POLICY

Background

The Itínere Group Compliance Unit has resolved to approve this corporate policy, which will apply generally to the Group companies, as part of its regulatory compliance programme, in response to the requirements of the European Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation); and of the Personal Data Protection and Guarantee of Digital Rights Act (Basic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights), in technical, legal and organisational terms.

This Policy aims to promote and maintain a responsible and proactive attitude towards personal data protection, in order to guarantee good personal data governance and preserve our stakeholders' trust.

Data protection governance model

The Itínere Group data protection governance model responds to the organisational requirements laid down by data protection regulations, by assigning and defining the data protection-related responsibilities and duties of the organisation's units and members.

The following aspects (among others), have been taken into account in devising the model:

- The appointment of a Data Protection Officer (DPO) in the Group and in each of its subsidiaries, who is responsible for ensuring compliance with current data protection regulations and for liaising with the data protection supervisory authority.
- The Data Protection Officer forms part of the Itínere Group Compliance Area, which will support the DPO to ensure that the data protection compliance system works properly, and submits recommendations regarding legal, technical and organisational improvements to the system to the Itínere Group Compliance Unit.

Developing the privacy culture

Awareness raising and training are key factors for developing a privacy culture within our organisation.

The Itínere Group promotes the data protection compliance system by involving its members in appropriate training, awareness-raising and sensitisation on how important the compliance system is within the Organisation's integrity culture.

The Itínere Group believes that having a corporate compliance culture is essential to ensure that everyone in the Organisation values stakeholders' and its members' right to privacy.

Proactive personal data protection

The Itínere Group takes a conscious, diligent and proactive approach to its personal data processing activities.

Accordingly, the Company has:

- This privacy policy, which outlines issues such as how personal data are processed, guarantees data subjects' rights, and data security.
- A specific personal data processing risk analysis methodology for assessing these risks and establishing security measures and controls for guaranteeing citizens' rights and freedoms.
- A methodology for identifying, assessing, classifying and responding to data protection regulation compliance-related security incidents.
- A data protection right protocol regarding the right to access, rectify and erase personal data (the right to be forgotten), to object to and restrict personal data processing, and data portability rights.

The Data Protection Officer is the person responsible for ensuring the protection of personal data protection rights within the Itínere Group. Our Data Protection Officer can be contacted by email: dpd@grupoitinere.com

Privacy policy

In compliance with the provisions of national personal data protection legislation and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, GDPR), you are hereby informed of how we will process your personal data.

This Privacy Policy will apply to all data processing performed by the Group's companies.

1. Purpose

This Personal Data Protection Policy forms part of the Group's Corporate Governance System and sets out the common personal data protection-related principles and guidelines that must govern the system and always guarantee compliance with applicable legislation. In particular, this Corporate Policy is intended to guarantee the data protection rights of any individuals who have dealings with the Group, ensuring respect for the right to honour and privacy in the processing of the different kinds of personal data that may be processed.

2. Scope of application

This Corporate Personal Data Protection Policy will apply to the Itínere Group, including its directors, managers and employees, as well as to everyone who has dealings with the Group's companies. By way of exception, any companies not wholly owned by the Group and which have their own personal data protection policy, as well as their respective subsidiaries, will be

excluded from the scope of application of this Personal Data Protection Policy. In either case, these companies' policies will include the mechanisms necessary to guarantee adequate personal data protection coordination with the rest of the Group. The representatives of any companies or entities in which the Company has a direct or indirect holding and that do not form part of the Group will ensure that the provisions of this Personal Data Protection Policy are observed and will, as far as possible, foster the application of its principles.

3. Personal data processing principles

The Personal Data Protection Policy is governed by the following principles:

a) General principles:

The Group companies will scrupulously comply with current data protection legislation and will ensure that the principles set out in this Corporate Policy are taken into account (i) in the design and implementation of all procedures involving the processing of personal data, (ii) where applicable, in the products and services offered by them, (iii) in any contracts and obligations they enter into with individuals and (iv) in the implementation of any systems and platforms that allow employees or third parties to access personal data and/or collect or process such data.

b) Personal data processing-related principles:

(i) Principles of legitimacy, lawfulness and loyalty in processing personal data. Personal data processing will be loyal, legitimate and lawful, in accordance with applicable law. In this regard, personal data must be collected for one or more specific and legitimate purposes in accordance with applicable law. Whenever it is mandatory under applicable law, the consent of the data subjects must be obtained before their data are collected. Furthermore, where required by law, the purposes for which personal data are processed must be explicit and determined at the time of being collected. In particular, the Group companies will not collect or process personal data concerning ethnic or racial origin, political ideology, religious or philosophical beliefs or convictions, sexual life or orientation, trade union membership, health, or genetic or biometric data intended to identify a person uniquely, unless the collection of such data is necessary, legitimate, and required or permitted by applicable law, in which case they will be informed of both the collection and the processing of the data in accordance with the law.

(ii) Data minimisation principle. Only those personal data that are strictly necessary for the purpose for which they are collected or processed and suitable for that purpose will be processed.

(iii) Data accuracy principle. Personal data must be accurate and kept up to date. Otherwise, they must be erased or rectified.

(iv) Storage period limitation principle. Personal data will not be kept longer than the period necessary to achieve the purpose for which they are processed, except in the cases provided for by law.

(v) Principles of integrity and confidentiality. Technical or organisational measures must be in place to ensure that personal data are processed with appropriate levels of security to protect

them from unauthorised or unlawful processing and to prevent their loss, destruction or accidental damage.

The personal data collected and processed by the Group's companies must be kept in the strictest confidence and secrecy, and may not be used for purposes other than those for which their collection was justified and allowed. Nor may they be disclosed or transferred to third parties except as permitted by applicable legislation.

(iv) Proactive responsibility (accountability) principle. The Group's companies must assess the risk posed by their data processing activities, in order to determine the measures to be applied to ensure that personal data are processed in accordance with legal requirements. Whenever so required by law, personal data protection risks must be assessed beforehand, and the necessary measures shall be taken to eliminate or mitigate them.

The Group's companies must keep an activity log that describes the personal data processing carried out in the context of their activities.

In the event of an incident that causes the accidental or unlawful destruction, loss or alteration of personal data, or the unauthorised disclosure of or access to such data, the internal protocols established jointly for this purpose by the Compliance Area and Systems Department, and any others established by the applicable legislation, must be followed. These incidents must be documented, and measures must be adopted to solve and mitigate any possible negative effects for the interested parties.

In the cases provided for by law, one or several data protection officers will be appointed in order to ensure compliance with data protection regulations in the Group's companies.

(vii) Transparency and information principles. Personal data processing will be transparent for the data subjects, who will be given information on the processing of their data in an understandable and accessible manner, when so required by the applicable law.

The Group company responsible for the processing will inform the data subjects or interested parties about: the identity of the company, area or body responsible for collecting the data; the origin and purpose of the data processing; the third parties or categories of third parties to which the data might be transferred; the legal grounds for the processing; profiling; the intention to carry out international transfers, if any; the data retention period; their personal data rights processing; the Data Protection Officer's contact details; their right to contact the competent supervisory authority.

The Itínere Group will only collect information and process personal data pursuant to the requirements established by the legislation applicable to each case regarding the purpose for which it is collected.

(viii) Acquisition or collection of personal data. The acquisition or obtaining of personal data from unlawful sources, from sources that do not sufficiently guarantee their lawful origin or from sources whose data have been collected or transferred in contravention of the law is prohibited.

(ix) Contracting of data processors. Before contracting any service provider who accesses personal data for which the Group companies are responsible, and throughout the term of the contractual relationship, the latter will adopt the measures necessary to guarantee and, when legally required, demonstrate that the data processor performs the data processing in accordance with applicable regulations.

(x) International data transfers. Any processing of personal data subject to European Union law that involves a transfer of data outside the European Economic Area must be carried out in strict compliance with the requirements established in the applicable law in the jurisdiction of origin.

c) The workplace: spearheading the defence of personal data protection within the Itínere Group.

The workplace is where the Itínere Group's human capital does its work every day, and as part of their daily tasks, all users need to access different systems and handle different types of information. Accordingly, we must bear in mind that the workplace is a key point from an information security perspective. To this end, the Itínere Group considers it necessary to apply a set of security measures to guarantee that all electronic and paper format information is correctly protected. In addition to the provisions of the Itínere Group's Computer Equipment and Device Use Policy:

c.1) Basic documentation management principles:

i.i.- Store or keep our information in a suitable location. Avoid keeping it close to cooling systems, water pipes or any facilities liable to affect paper.

i.ii.- Use suitable paper storage elements, such as cupboards and drawers with locks, or fireproof safes or cabinets if necessary.

i.iii.- Destroy documentation safely and securely. Depending on the volume of paper, we can use conventional paper shredders or have the paper removed and destroyed by the approved supplier contracted for this purpose.

i.iv.- Clean tables. Every day we work with a large amount of documentation. Workstations must be kept clear, and only the material that is required for the task being performed at any given time must be left on the table. Sensitive information must not be left where people who might misuse it can see it. Compliance with this policy involves: keeping workstations clean and tidy; putting away documentation and removable devices that are not being used at the time, especially when absent from workstations or at the end of the working day; not writing down usernames or passwords on post-its or similar.

c.2) Workplace protection:

i.i.- Employees must act in accordance with the provisions of the Itínere Group's Information Security policy, its Code of Conduct, the IT resource use policy, and any other applicable internal policies.

i.ii.- Documents must be destroyed using the secure mechanisms provided, namely paper shredders or by the secure external destruction service.

i.iii.- Session blocking. Whenever users leave their workstation, they must block their computer terminal session.

4. Implementation

In line with the provisions of this Corporate Personal Data Protection Policy, the Compliance Area will develop and keep up to date the Group's internal global data management protection regulations, which will be implemented by the Systems Department and will be binding on all of the Group's executives and employees.

The Compliance Area will be responsible for reporting to the Compliance Unit on any developments and new regulations in this regard.

The Systems Department, or whichever area takes on its duties in the Group companies, will be responsible for ensuring that any IT developments and controls required to guarantee compliance with the internal global management data protection regulations are implemented in the information and will ensure that these developments are updated from time to time. In addition, all the Itínere Group companies must:

(i) Designate the person responsible for processing personal data in their sphere of activity, who will liaise with and act under the supervision of the data protection officer.

(ii) Coordinate any activity that involves or entails handling personal data with the Systems Department.

Finally, the Compliance Unit will monitor the general state of personal data protection in the Group's companies and ensure that personal data protection risk management and practices are coordinated properly throughout the Group, assisting the Data Protection Officer and the Systems Department in the approval of internal regulations in this regard.

5. Monitoring and evaluation

(I) Monitoring: The Compliance Area is responsible for supervising compliance with the provisions of this Corporate Personal Data Protection Policy by the Company and the other Group companies, although other bodies and departments of the Company and the rest of the Group's companies are also responsible for doing so.

Compliance with this Corporate Personal Data Protection Policy may be verified by conducting internal or external audits at regular intervals.

(ii) Evaluation and updates: At least once a year, the Compliance Unit will assess compliance with and the effectiveness of this Corporate Protection Personal Data Policy and will report the result to the Company's governing body.

This Policy must be kept up to date over time, by being reviewed ordinarily once a year, and extraordinarily whenever there are changes to the strategic objectives or applicable legislation. Any proposed modifications will be put forward by the Compliance Area, after consulting the Compliance Unit, which will, if appropriate, submit it to the Board for approval.