FTI GROUP

FTI GROUP

DATA PRIVACY POLICY ("DPP")

Group Policy

Department:	Governance & Compliance | Data Protection
Prepared by:	Kerstin Einer, Stephan Kistler
Document-No.:	[DP-2023-01]
Issue/Revision:	1.0
Creation Date:	20.01.2023

Marc Waeber	Ralph Schiller
Chief Governance & Compliance Officer	Chief Executive Officer
Marc Waeber	
Signature	Signature

WE PROTECT
PERSONAL DATA

Foreword

The protection of Personal Data and the respect for privacy are fundamental European rights and are also becoming increasingly important worldwide. In Europe, a new chapter in data protection began with the General Data Protection Regulation (GDPR) entering into force on **May 25, 2018.** High standards to the Processing of Personal Data also apply in many countries outside the European Union and the European Economic Area.

FTI GROUP is an addressee of the GDPR and various national data protection laws worldwide that must be observed when handling Personal Data. Violations of these regulations can result in high fines by data protection authorities.

As a tourism group, FTI GROUP processes Personal Data of Employees as well as those of partners and customers (travellers, hotel guests, air passengers, etc.), who may rely on us handling this data carefully and process it in compliance with the law. Therefore, the protection of Personal Data is not only a legal obligation, but also a key element in maintaining trust in FTI GROUP as an employer, in our products and in us as a business partner. Misuse of Personal Data and information can seriously damage the reputation of FTI GROUP and result in both fines from authorities and financial losses due to the loss of trust of our partners and customers.

In our Code of Conduct, we have therefore committed ourselves to comply with Applicable Data Protection Laws and with our own policies and guidelines on data protection and data security when collecting and Processing Personal Data. This Data Privacy Policy sets out our worldwide minimum standard for handling Personal Data and regulates which principles must be observed by each individual FTI GROUP company, its executives and all Employees when Processing Personal Data.

Table of Contents

A. Scope of Application and Objective of the Data Privacy Policy

I. Applicability

This Data Privacy Policy (hereinafter "**DPP**") applies to:

1) all FTI GROUP companies established in the European Union (EU) and European Economic Area (EEA), their executives and Employees and extends to all Processing of Personal Data carried out by those FTI GROUP companies whether relating to Employees, customers, business partners or other Data Subjects, regardless of whether the Processing takes place in the EU/EEA or not;

2) all FTI GROUP companies not established in the European Union, their executives and Employees insofar as they Process Personal Data of Data Subjects who are in the EU/EEA and the Processing is related to:

   - the offering of goods or services in the EU/EEA, irrespective of whether a payment of the Data Subject is required (whether goods or services are offered in the EU is determined by whether the company acting as Controller or Processor has an obvious intention to offer the goods or services to Data Subjects in one or more EU member states); or
   - the monitoring of Data Subjects' behaviour as far as their behaviour takes place within the EU/EEA.

II. Objective

The aim of this DPP is to create minimum organisational standards for the handling and Processing of Personal Data at FTI GROUP and to establish a uniform framework for the Processing and protection of Personal Data. This DPP serves as a framework policy on data protection and may be from time to time supplemented by guidelines and best practices on specific subject matters, such as:

- Data Protection Impact Assessment (DPIA) Guideline;
- Data Breach Response Guideline;
- Guideline on Protecting Data Subjects' Rights.

The FTI GROUP companies, their executives and Employees, are each responsible for complying with this DPP and Applicable Data Protection Laws.

Individual FTI GROUP companies are not entitled to establish any regulations or provisions that diverge from this DPP unless these regulations impose stricter requirements for the handling of Personal Data.

If there is reason to assume that **statutory obligations are in conflict** with the duties arising under this DPP, then the competent Data Protection Officer or Data Protection Coordinator is to be notified without delay.

In the event of discrepancies or inconsistencies, except as expressly permitted in this DPP or stipulated with reference to the overridden DPP in a guideline or best practice document, between the DPP and the guidelines, the DPP shall have higher priority.

Unless specifically mentioned otherwise, the provisions and definitions of this DPP apply to the mentioned guidelines and best practices mutatis mutandis.

B. Definitions

The following definitions apply:

- **"Anonymisation"** means the process of rendering Personal Data anonymous. Anonymous data is information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
- **"Applicable Data Protection Laws"** means GDPR and any national laws on data protection applicable to each FTI GROUP company insofar as these laws are applicable to the Processing of Personal Data of citizens of the European Union (EU) and the European Economic Area (EEA).
- **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- **"Data Protection Office"** means the central data protection department within group function "Governance and Compliance" at FTI Touristik GmbH.
- **"Data Protection Officer"** means an internal or external data protection expert officially appointed by one or more FTI GROUP companies where it is required by Applicable Data Protection Laws.
- **"Data Protection Coordinator"** means a designated data protection expert and can be appointed for individual companies, business units or departments of the FTI GROUP.
- **"Data Subject"** (see "Personal Data").
- **"DPA"** means Data Processing Agreement as set out in Article 28 GDPR - see section E.II.1.
- **"DPIA"** means Data Protection Impact Assessment as set out in Article 37 GDPR - see section E.VII.
- "**DPPO**" means Data Protection Process Owner – see section F.II.
- **"Employee"** means an employee within the meaning of section 26 (8) of the German Federal Data Protection Act (BDSG) or any other applicable national law, in particular an employee or person who is to be regarded as person that is like an employee on account of his or her lack of economic independence.

- **"FTI GROUP"** means FTI Touristik GmbH and its subsidiaries as defined in section 15 ff. of the German Stock Corporation Act (AktG) and companies associated with FTI Touristik GmbH such as EUVIA TRAVEL GmbH.

- **"GDPR"** means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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).

- **"Joint Controllership"** means a relationship where two or more Controllers jointly determine the purposes and means of the Processing of Personal Data - see section E.III.

- **"Personal Data"** means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, email address, an identification/booking 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; customer and partner data in this regard belong to Personal Data as much as data about Employees. For instance, the name of a contact person permits conclusions about a natural person just as much as such a person's email address. It is sufficient for the respective information to be tied to the name of the Data Subject or for connections to be able to be established with the Data Subject apart from this. Likewise, a person may be identifiable if the information first needs to be linked to additional knowledge. Photos, videos, or audio recordings, GPS position data, server log files, or a tax identification number therefore may also be Personal Data.

- **"Processing"** means 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.

- **"Processor"** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

- **"Pseudonymisation"** means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to Technical and Organisational Measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person.

- **"Recipient"** means a natural or legal person, authority, institution or other body to which Personal Data is disclosed.

- **"Records of Processing Activities"** means the records listing all Processing activities carried out by a FTI GROUP company, containing at least the information set out in Article 30 GDPR.

- **"Special Categories of Personal Data"** means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Special Categories of Personal Data are also genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- **"Technical and Organisational Measures"** ("TOMs") means measures designed to contribute to and promote the security of the Processing of Personal Data. They comprise a bundle of the most diverse instruments with which companies can ensure the protection of Personal Data.

- **"Third Country"** means all states outside the European Union (EU) and the European Economic Area (EEA).

- **"Third Party"** means a natural or legal person, authority, institution or other body, except for the Data Subject, the Controller(s), the Processor(s), and the individuals who are subject to the direct responsibility of the Controller(s) or of the Processor(s) and authorized to Process the Personal Data (this may also include, for instance, freelancers).

- **"(Data) Transfer"** means the process of disclosing data, including sharing, enabling access to the data and otherwise making data available.

C. Designation of Data Protection Officers and Data Protection Coordinators

The legal representative of each FTI GROUP company (e.g. the managing director) is and always remains accountable for ensuring compliance with Applicable Data Protection Laws within the respective company.

Appointed Data Protection Officers and Data Protection Coordinators – as set out in section I. and II. below – must be reported to the Data Protection Office at FTI Touristik GmbH to maintain a list of contacts at the *Data Protection Sharepoint* (https://ftigroup.sharepoint.com/sites/DataProtection).

I. Data Protection Officers

Each FTI GROUP company which is required to have an official **Data Protection Officer** under Applicable Data Protection Laws must appoint an internal or external data protection expert as Data Protection Officer.

II. Data Protection Coordinators

In addition to the Data Protection Officers, **Data Protection Coordinators** can be appointed for individual companies, business units or departments of the FTI GROUP.

Each FTI GROUP company that processes Personal Data on a regular basis and has no legal obligation to have a Data Protection Officer must appoint a Data Protection Coordinator.

Each Data Protection Officer and each Data Protection Coordinator works to ensure compliance with Applicable Data Protection Laws and to monitor compliance with this DPP within its area of responsibility.

In addition, the Data Protection Officers and Data Protection Coordinators are responsible for reporting at regular intervals on the compliance with Applicable Data Protection Laws relevant to their area of responsibility.

D. Principles for Processing Personal Data

Principles for Processing Personal Data can be found in the national laws of most countries, either in comprehensive data privacy laws or in other laws. Whenever Personal Data is being Processed by an FTI GROUP company as a Controller, the relevant FTI GROUP company is responsible for complying with these principles and in particular with the principles described below which may differ from obligations postulated by the applicable national law of the respective company.

Each FTI GROUP company must be able to prove compliance with below principles.

I. Lawfulness

Personal Data must be collected and Processed in a lawful manner and on a legal basis prescribed by Applicable Data Protection Laws.

II. Fairness

Personal Data must be Processed in good faith and in a manner that is fair to the Data Subject. The respective Data Subject is not to be deceived or misled when collecting Personal Data. The collected data will only be handled in ways the Data Subject would reasonably expect or where any unexpected Processing can be justified.

III. Transparency

Personal Data may be Processed only in a manner that can be comprehended by the Data Subject. Information and communication about the Processing must be easily accessible and easy for the Data Subject to understand, using clear and plain language.

IV. Purpose limitation

Personal Data may be Processed only for clear and legitimate purposes that have been determined before the data is Processed. Therefore, Personal Data must not be collected if there is no specified, explicit and legitimate purpose for the collection of these Personal Data. Subsequent changes to the identified purposes of Processing are possible only in limited cases and require a justification.

V. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which they are Processed. Before Personal Data is Processed, it is necessary to carry out a review as to whether and to what extent such Processing is necessary in order to achieve the goal that is being pursued by means of the Processing.

Personal Data must be reasonable and significant for the purpose and must be limited to the amount needed for the purposes of Processing. If it is possible to achieve the goal and the effort is reasonably proportionate to the goal pursued, then anonymized data shall be used. Personal Data may not be stored only to ensure availability for potential future purposes unless this is prescribed or permitted by the Applicable Data Protection Laws.

VI. Accuracy and data currency

Personal Data is to be stored accurately, completely, and in an up-to-date state. Reasonable measures are to be taken to ensure that inaccurate, incomplete, or old data is erased, rectified, supplemented, and/or updated without unreasonable delay.

VII. Storage limitation and erasure

Personal Data may be stored in a form that enables identification of the Data Subjects only for as long as needed for the purposes for which they are Processed unless the storage is otherwise required by applicable national law e.g. retention periods in national/EU tax or accounting laws.

Personal Data that are no longer needed after expiration of statutory retention periods or retention periods having to do with business processes must be erased – unless it is permitted to keep them in the particular case after conferring with the responsible Data Protection Officer or Data Protection Co-ordinator.

If you intend to **retain Personal Data after the expiration of the retention periods**, please notify the competent Data Protection contact of your FTI Group company in advance.

VIII. Integrity and Confidentiality

The principle of integrity and confidentiality requires adequate protection and appropriate security of Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction or damage.

During the Processing of Personal Data, appropriate Technical and Organisational measures based on the risk of the respective Processing and the sensitivity of the data must be taken to ensure adequate security of the Personal Data.

If you have **questions or concerns** in connection with the Processing of Personal Data, please contact the competent Data Protection contact of your FTI Group company.

E. Rules of Conduct / Specifications

The aim of this DPP is to create minimum organisational standards for the handling and Processing of Personal Data at FTI GROUP and to establish a uniform framework for the Processing and protection of Personal Data. This DPP serves as a framework policy on data protection and is supplemented by FTI GROUP's data protection guidelines and best practices on specific subject matters.

I. Permissibility of the Processing

The Processing of Personal Data is lawful only if and to the extent that there is a specific legal basis. Such a reason for permission is also necessary whenever the purpose for the Processing of Personal Data is intended to be changed from the originally stated purpose.

The Data Protection Process Owner´s ("DPPO") – see section F.II.1 below – are responsible to proof compliance with the requirements laid down in the **Legitimacy of Processing Activities Guideline** at all time. The Legitimacy must be demonstrated before a new Processing Activity may be started.

Basic principle: Any Processing of Personal Data is generally prohibited, unless the requirements of a legal basis for the Processing are fulfilled.

Whenever Processing of Personal Data falls within the scope of the GDPR, it is permitted only if a reason for permission exists. This is particularly the case where:

- the Processing is necessary for the **performance of a contract** to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- the Processing is necessary for **compliance with a legal obligation** to which the Controller is subject;
- the Data Subject has given **Consent** to the Processing of his or her Personal Data for one or more specific purposes;
- the Processing is necessary for the **purposes of the legitimate interests** pursued by the Controller or by a third party, except where such interests are overridden by the interests of the Data Subject.

Special attention must be paid to the Processing of Special Categories of Personal Data according to Article 9 GDPR as well as for the Processing of Personal Data of Employees.

1. Special Categories of Personal Data

The Processing of Special Categories of Personal Data is lawful under the provisions of Article 9 (2) GDPR - in particular, if one of the following cases are given:

- the Data Subject has given **explicit consent** to the Processing of those Personal Data for one or more specified purposes after being informed about the especially protectable nature of the data;
- the Processing relates to Personal Data which are manifestly **made public** by the Data Subject

2. Personal Data of Employees

For specific Processing situations, e.g. Processing in the context of employment, the GDPR provides exceptional provisions which allow the Member States to regulate the legal basis for the Processing of Personal Data in national law.

The Processing of Personal Data is lawful if the requirements of such a legal basis are fulfilled.

II. Transfers of Personal Data

Most data privacy laws impose specific requirements for Transfers of Personal Data to other legal entities which can either be Third Parties or other FTI GROUP companies. A Transfer of Personal Data happens when personal information is disclosed or transmitted, including possible remote access to Personal Data.

The DPPO is responsible to fulfil the requirements set forth in the sections below as specified in the FTI Group's **Data Transfer Guideline**.

1. Transfers to Third Parties

Any Transfer of Personal Data to Third Party Recipients is subject to the permissibility requirements for the Processing of Personal Data (see section E.I above) or in case the Transfer does not fall within the applicability of the GDPR to the respective applicable national law.

The Controller remains accountable for ensuring that the Processing by the Processor is compliant with GDPR and other Applicable Data Protection Laws. Therefore, the Recipient of the data must be obliged to use such data only for the agreed purposes.

Processing must be performed on a contractual basis whenever a contractor is engaged to Process Personal Data as a Processor without transferring responsibility to such contractor for the related business process. In such cases, it is necessary to enter into a **Data Processing Agreement ("DPA")**.

Typical examples for Controller-Processor relationships:

- IT service providers, especially for storage; SaaS or other cloud or managed services; maintenance with access to Personal Data.
- Payroll service providers.

- Call centre service providers.
- Storage devices (hard drives, flash drives etc.), data or document disposal.
- Hardware, but only if the seller or manufacturer provides connected data services (e.g. IoT devices, other devices that collect Personal Data and offer connectivity to storage or managed services).

Before a contractor begins Processing of Personal Data, a Data Processing Agreement ("DPA") must be concluded.

In doing so, the engaging company will maintain responsibility for ensuring that the Processing takes place in a manner that is compliant with Applicable Data Protection Laws. The Processor may Process Personal Data only within the context of the instructions given by the engaging company as Controller. With regard to the granting of the assignment and entering into the DPA, the regulations set forth in Article 28 GDPR are to be observed; the department at the FTI GROUP company engaging the Processor must ensure implementation.

2. Transfers by Third Parties

In the event of data transfers by Third Parties to FTI GROUP companies, it is necessary to ensure that the data is used for the envisioned purposes.

3. Transfers from the EU/EEA to Third Countries

In the event of a data Transfer from the EU/EEA to a Recipient in a Third Country, this Recipient must guarantee an adequate level of data protection that is equivalent to the level of protection granted within the EU.

If a **transmission of Personal Data to a Recipient in a Third Country** is planned, then the competent Data Protection Officer or Data Protection Coordinator shall be notified in advance.

Articles 44 to 49 GDPR cover how an adequate level of data protection can be ensured.

First of all, a Transfer of Personal Data to a Third Country may be carried out if the European Commission has determined by means of an adequacy decision that a reasonable level of data protection prevails in the relevant Third Country (for instance, Switzerland, Canada, UK or Israel).

If there is no adequacy decision applicable to the relevant Third Country, suitable guarantees must be in place for an adequate level of data protection. These may consist of, for instance, binding internal data protection provisions (binding corporate rules) or EU Standard Contractual Clauses. Exceptional cases in which data transfers can still be permitted are listed in Article 49 GDPR.

III. Joint Controllership

If two or more Controllers of which at least one is an FTI GROUP company jointly determine the purposes and means of Processing, they qualify as joint controllers.

In such cases, the joint controllers are to conclude a **Joint Controller Agreement**, which determines their respective responsibilities for compliance with the obligations under the GDPR in accordance with Article 26 GDPR.

IV. Data Transfers within the FTI GROUP

To comply with the requirements outlined in sections E.II and E.III above, the FTI GROUP companies shall enter into an **Intra-Group Data Transfer Agreement** ("**IDTA**").

An IDTA serves to ensure that the contractual requirements for intra-group data transfers are regulated uniformly throughout the FTI GROUP, thereby further contributing to the achievement of a uniformly high level of data protection throughout the FTI GROUP.

Each FTI GROUP company can decide for itself whether to access the IDTA. Both the time of accession to and potential termination of the IDTA by a FTI GROUP company are at the sole discretion of the relevant company. For companies that are not yet part of the FTI GROUP, this applies from the time of they become members of the FTI GROUP.

However, exiting the FTI GROUP automatically leads to the termination of the IDTA.

V. Notification to the Data Subject

Information about the Processing in accordance with Articles 13 to 14 GDPR shall be provided to the Data Subject in a precise, transparent, comprehensible, and easily accessible form in clear and simple language.

The information will be provided to the Data Subject either:

a) in the case of **customers and partners** within the context of entering into a contract;

b) in the case of **Employees** - through the Privacy Notice for Employees which is provided to the Employees at the latest when entering into the employment agreement; or

c) in the case of **website visitors** - by means of a Privacy Notice for Websites that is prepared for each website individually and available on the relevant website.

The DPPO must comply with transparency and information requirements set out in Article 12 to 14 GDPR and the **Transparency and Information Guideline**.

VI. Rights of the Data Subjects

Each Data Subject can exercise the rights described below in sections E.VI.1 to E.VI.5. The assertion of such rights by a Data Subject must be immediately processed, and any such assertion may in no way lead to any disadvantages for the Data Subject.

If a **Data Subject makes use of one of its rights**, as enumerated below, each employee is obliged to immediately report the request in conformity with the **Guideline on Protection of Data Subjects' Rights** of the FTI GROUP.

1. Right to access

The Data Subject has the right to demand confirmation from the Controller whether Personal Data concerning the Data Subject is being Processed. If the Data Subject's Personal Data is being Processed, the Data Subject has a right to access this Personal Data.

2. Right to rectification, limitation of Processing, and erasure

The Data Subject has the right to demand that the Controller immediately rectifies inaccurate or erases Personal Data concerning the Data Subject or, possibly, to limit the Processing of Personal Data.

3. Right to data portability

The Data Subject has the right to obtain the Personal Data concerning themselves, which they have provided to a Controller, in a structured, commonly used, and machine-readable format, and – subject to the conditions set forth in Article 20 GDPR – they have the right to transfer this data to another Controller.

4. Right to object

The Data Subject has the right to object to the Processing of Personal Data concerning themselves that takes place (i) on the basis of Art. 6 (1) (f) GDPR, or (ii) for the purpose of direct advertising. The Data Subject must be expressly notified of its right to object no later than at the time of initial communication.

5. Right to appeal

Every Data Subject has the right to file an appeal with a supervisory authority in connection with the Processing of its Personal Data. The Data Subject is to be notified of this option.

VII. Data Protection Impact Assessments

If a form of Processing of Personal Data is likely to present a high risk to the rights and freedoms of Data Subjects, each Processing department of the applicable company(ies) of the FTI GROUP are required to carry out a Data Protection Impact Assessment ("**DPIA**") of the intended Processing, in advance.

The DPIA shall comply with the minimum requirements set out in Article 35 (7) GDPR and the **Data Protection Impact Assessment (DPIA) Guideline**.

The competent Data Protection Officer or Data Protection Coordinator shall be consulted and provide advice and support to the Processing department(s) for the purpose of conducting the DPIA, primarily for the determination of a high risk of Processing.

VIII. Security of Processing

Personal Data is to be protected at all times from unauthorized access, unlawful Processing, loss, falsification, or destruction. This applies regardless of whether the Processing is carried out electronically or in paper form.

Before the introduction of new procedures for the Processing of Personal Data, in particular new IT systems, adequate Technical and Organisational Measures are to be determined and implemented. These measures have to be based on state-of-the-art technical standards, the risks proceeding from the Processing, and the need for protection of the Processed Personal Data.

The department responsible for introducing a new procedure, before introducing the procedure, shall ask the IT Security Officer and the competent Data Protection Officer or Data Protection Coordinator for support in developing the security concept of the procedure.

IX. Personal Data Breach

Any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed is to be treated as a Personal Data Breach.

GDPR requires identification and mitigation of Data Breaches as well as notification to supervisory authorities, Data Subjects such as Employees or customers, depending on a risk assessment. Any notification must be made without undue delay and notifications to supervisory authorities within 72 hours at the latest. Immediate action is therefore required by all Employees in case of a Data Breach.

Employees are obliged to **immediately report a possible Personal Data Breach** in conformity with the **Data Breach Response Guideline** of the FTI GROUP.

X. Confidentiality of the Processing and Data Secrecy

1. Confidentiality/Unauthorized Processing

Employees are prohibited from engaging in **unauthorized Processing** of Personal Data. Unauthorized Processing is any Processing that an Employee carries out without being assigned this task within the context of performing its duties and/or without being appropriately entitled to do so.

The need-to-know principal applies: Employees may obtain access to Personal Data only if and to the extent this is necessary for their respective duties. This requires the diligent apportionment and separation of roles and responsibilities as well as the implementation and maintenance of them as part of the authorization concepts.

Employees may not use Personal Data for their own private or economic purposes, transfer them to unauthorized parties, or otherwise make them accessible to unauthorized persons.

2. Data Secrecy

Supervisors must inform their Employees at the start of the employment relationship about the duty to uphold data secrecy. Employees are to be obliged in writing to data secrecy when starting their work. The commitment to data secrecy forms part of the employment agreement of each FTI GROUP company and is to be provided to Employees in the relevant language of the employment agreement at latest when it is signed. This obligation to uphold data secrecy will exist even after the employment relationship has ended.

F. Responsibilities

I. Management

The management of each FTI GROUP company is accountable for implementing this DPP and for compliance with the applicable statutory obligations.

Each member of the management has to ensure that managers, Employees and any Third Parties who work with Personal Data on behalf of the relevant FTI GROUP company are informed about FTI GROUP data protection standards and, to the extent necessary, trained in observing them.

The duties and responsibilities involved in handling Personal Data – as outlined in sections D und E – is to be clearly defined, routinely monitored, and documented.

Each member of management is obliged to support the Data Protection Officer or Data Protection Coordinator in their activities and provide the requested necessary information without undue delay.

II. Departments

The head of each department processing Personal Data is responsible for complying with the Applicable Data Protection Laws and requirements set out in the data protection guidelines published by FTI GROUP, however he/she may delegate responsibilities to the person responsible for a certain Processing of Personal Data ("Data Protection Process Owners").

1. Data Protection Process Owners

The Data Protection Process Owner´s ("DPPO") core role is to ensure the legitimacy of standardized Processing activities within his/her area of responsibility. This task is limited to the compliance of such processes with the requirements of the GDPR, applicable local data privacy laws and all relevant Company privacy policies and guidelines.

The Data Protection Process Owner should not be confused with the Application Owner – as set out below -, who is responsible for the application (computer program designed for a specific task or use) used in the Processing activity. It is possible that a Processing is supported by more than one application or also includes paper-based Processing.

2. Application Owners

For applications that require particular support with regard to Applicable Data Protection Laws, an **Application Owner** is to be appointed by the head of the competent department who works in operations and functions as an internal contact person for topics concerning Applicable Data Protection Laws.

Such applications are generally:

- websites and apps,
- IT systems and software, in which large quantities of end customer data is Processed (customer and user administration, CRM),
- the administration of consent (opt-ins) and objections as well as
- the Processing of Employee data, health data, bank/credit card data, or other particularly sensitive data.

The Application Owner is obliged to cooperate with the Data Protection Process Owners and competent Data Protection Officer or Data Protection Coordinator in connection with the administration and updating of the Records of Processing Activities and provide the necessary information.

The heads of departments or Data Protection Process Owners, who are responsible for business processes and projects, must notify the competent Data Protection Officer or Data Protection Coordinator in due time **before the introduction of any new Processing** of Personal Data.

G. Data Protection Checks

Compliance with this DPP and the Applicable Data Protection Laws shall be reviewed at least annually by means of internal data protection audits and further checks. The competent Data Protection Officer or Data Protection Coordinator or engaged external auditors will bear the responsibility of carrying this out.

The results of the data protection checks are to be communicated to the competent members of management and to the Data Protection Office at FTI Touristik GmbH.

The risks associated with Applicable Data Protection Laws including associated reputational risks must be compiled by management at least once a year and must be evaluated with regard to possible impact on business processes. The results of the risk analysis must be documented and, in so far as they are essential to the FTI GROUP, included in the central risk management system.

The competent Data Protection Officer or Data Protection Coordinator is to be notified immediately in the event that supervisory authorities carry out any data protection controls.

H. Data Privacy Trainings

Employees of every FTI GROUP company whose activities involve the Processing of Personal Data shall receive training on data protection topics at the beginning of their employment and on a regular basis thereafter.

In order to undertake the training, Employees must attend the training on data protection provided by the respective FTI GROUP company via intranet or other platforms. The completion of each training course must be documented.

I. Compliance with this DPP

A negligent or even wilful violation of this DPP may result in employment action, including termination with or without notice. Criminal sanctions and civil consequences such as compensation for damages are also possible.

Compliance with the requirements of this DPP must be verifiable by the respective FTI GROUP company at all times. In this context, particular attention must be paid to the traceability and transparency of measures taken, for example, by means of associated documentation.

J. Updating this DPP

This DPP will be routinely reviewed in terms of any need to adjust or supplement it as a result of any developments in the Applicable Data Protection Laws, technological or organisational changes and as a result of the outcomes of data protection checks. The Data Protection Office at FTI Touristik GmbH is responsible for initiating such reviews.

Any changes to this DPP are valid without any form requirement. The Employees and the management are to be notified of any changes immediately after the changes come into effect.

K. History

Edition	Date	Author	Change Description
1.0	20.01.2023	Kerstin Einer, Stephan Kistler	First version