ELIOR GROUP

Personal Data Protection Policy

Scope	All scopes
Version	V1
Written by	DCP Operational Committee
Approved by	DCP Steering Committee
Publication date	01/03/2019
Date updated	

Introduction

This personal data protection policy defines how the Elior Group proceeds when implementing personal data processing to ensure the protection of the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.

It defines the standards that all Elior Group employees, partners and processors must adhere to when processing personal data.

It should be noted that failure to comply with personal data protection obligations exposes the Elior Group to a penalty of 4% of its global turnover; for information purposes, this represents nearly €268 million based on the results for the financial year ended 30 September 2018.

Each of the persons concerned must in particular ensure:

- respect for the principle of privacy by design of new projects, and in particular that each data processing task (i) corresponds to a defined purpose, (ii) provides for informing the persons of the data processing implemented, (iii) determines protective measures and (iv) sets a retention period for personal data;
- compliance with the deadlines imposed to respond to requests to exercise rights, i.e. one month, and notification of any data leak to the competent authorities within 72 hours;
- more generally, compliance with the processes and recommendations put in place by this policy and the soliciting, if necessary, of the personal data protection ambassadors or the Elior Group GDPR team at gdpr-contact@eliorgroup.com.

Glossary

"**Elior Group"** means the company Elior Group and all companies that, within the meaning of Article L233-3 of the French Commercial Code,

(i) are under the direct or indirect control of the company Elior Group, or,

(ii) are, directly or indirectly, under common control with the company Elior Group;

"**data of a personal nature**", "**personal data"** or **"PD"** means any information relating to an identified or identifiable natural person (hereinafter **"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, 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;

"**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;

"**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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

"**processor"** means the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"**IS controller"** means the Elior Group employee, who is responsible for the technical knowledge relating to the IT resources involved in the processing task, for each personal data processing task identified within the Elior Group;

"**business needs manager"** means the employee within the Elior Group, who defines the business needs and the processing objectives (project management), for each data processing task identified within the Elior Group;

"**recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether or not this recipient is outside the Elior Group (third party). However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

"**consent**" [of the data subject] means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

"**personal data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"**binding corporate rules**" or "**BCR"** means an intra-Group data protection policy in connection with any transfer of personal data occurring in whole or in part outside the European Economic Area. They are legally binding and complied with by the entities that are signatories within a group of companies, regardless of their country of operation, as well as by all employees of the same legal entity or group of companies. There are two types of BCR: (i) the BCRs

"controller", which provides a framework for transfers made within a group acting as controller, and (ii) "processor" BCRs, which enable the creation of a security sphere for transfers made when the group acts as a processor;

"**data protection impact assessment**" or "**DPIA**" means that the controller shall, prior to any processing task that may give rise to a high risk to the rights and freedoms of natural persons, in particular through the use of new technologies, perform an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may relate to a set of similar high risk treatment operations.

Contents

1. Background

As a catering service provider, food safety is a fundamental aspect of Elior Group's business. Offering a healthy, well-prepared diet, that is distributed in accordance with the regulations in force to its customers and guests is a permanent concern for the Elior Group and is one of the foundations of the trust placed in it. In the same way, processing personal data in accordance with the legislation in force is a fundamental challenge for the Elior Group.

Indeed, the rapid evolution of technologies and globalisation have led to a substantial increase in exchanges of personal data between operators, which leads to new challenges for the protection of personal data. The extent of the collection and sharing of personal data has increased significantly, which promotes the unprecedented use and valuation of this data. The Elior Group, which aims to differentiate itself through technological innovation in the field of digital technology and an increasing capacity to collect and exploit data, is fully in line with this trend. Data are omnipresent and now positioned at the heart of the value creation chain. Well-managed and secure, they make it possible to increase efficiency and competitiveness, customise and strengthen relations with customers and guests, conquer new markets, improve products and services, and facilitate collaboration and mobility.

This cannot be achieved without establishing the trust that will enable the Elior Group's digital positioning to develop, by guaranteeing the teams, customers, guests and, more generally, all Elior Group contacts control of their personal data.

Given the emergence of national and supranational legislative frameworks, the Elior Group is constantly striving to adapt to the challenges of digital technology and is developing an approach based on continuous improvement and compliance for personal data management.

2. Scope

Elior Group's activities require it to constantly process personal data, for example:

- when capturing images using video surveillance cameras;
- when processing customer requests;
- when gathering guests' diets in order to serve them appropriate meals;
- or, when collecting information about the teams relating to the management of their careers.

This policy applies to all employees, partners and processors of the Elior Group each time that personal data relating to customers, guests, teams, suppliers or other natural persons are collected, used, made accessible or shared.

Given the location of the Elior Group's head office in France, this policy aims in particular to meet the obligations set out in 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 the free movement of such data, hereinafter referred to as the "General Data Protection Regulation", "Regulation" or "GDPR".

This approach is part of a desire to harmonise practices at Elior Group from the top down, to simplify the monitoring and maintaining of compliance over time and to guarantee a high level of personal data protection. In order to achieve this, this policy must, as far as possible, take account of national specificities:

- within the European Economic Area, in parallel with the General Data Protection Regulation, by compliance with specific national legislative provisions stating the conditions under which the processing of personal data is lawful;
- outside the European Economic Area, by taking into account, in all States in which the Elior Group is present, national legislation dedicated to the protection of personal data, or even an authority specifically competent for its application.

It must be made clear that the right to protection of personal data is not an absolute right, it must be considered in relation to its function in society and must be balanced against other fundamental rights, in accordance with the principle of proportionality, including respect for privacy and family life, home and communications, freedom of thought, conscience and religion, freedom of expression and information or freedom of enterprise. This policy does not seek to define the balance between these rights, which must be examined on a case-by-case basis by the Elior Group's legal departments with regard to changes in case law and the recommendations of the authorities.

3. Governance

A. General framework

The data management control approach is driven by a Group **team** composed of:

- A **Group Chief Compliance Officer** - reporting directly to the Chief Executive Officer, he/she is responsible for implementing compliance rules. He/she guarantees that the protection of personal data within the Elior Group is taken into account at an optimal level;

- A **Group Data Protection Officer** (DPO) - he/she guarantees the implementation of the personal data protection programme and compliance with the associated legislation for the entire Elior Group. He/she has in-depth knowledge of the Elior Group's business lines and organisation, in particular processing operations, information systems and the Elior Group's data protection and security needs. He/she carries out his/her duties and missions independently and can rely on a **Group IT Security Compliance Manager**.

- A **Group Senior Legal Counsel** - he/she assists and advises the DPO in the understanding and interpretation of legal texts and in the relationship with the personal data protection authorities. He/she also guarantees that personal data protection issues are taken into account in contractual relations.

The Group team relies on decentralised players in the Elior Group - the Personal Data **ambassadors**. These personal data ambassadors act as relays for the DPO within their scope and contribute in particular to:

- the construction of the associated policies and procedures;
- ensuring compliance with Group policy, in particular with respect to the exercise of rights and the keeping of the register of processing operations;
- be the preferred points of contact vis-à-vis the Group GDPR team and their scope for any questions relating to personal data.

This policy is revised on an annual basis, at the initiative of the Group GDPR team to take into account any changes in legislation or internal practices within the Elior Group. Each Elior Group subsidiary is free to organise itself internally and to define this policy in order to facilitate its dissemination and application.

B. Compliance tool

The Elior Group has recently obtained compliance management software to meet the obligations relating to the protection of personal data and to manage the associated procedures or to support its teams in so far as concerns adherence to the rules of compliance as part of their activities.

All Elior Group employees called upon to have responsibility for the processing of personal data (i.e. IS controllers and business needs managers and personal data ambassadors) have access to this environment. This tool is used in particular to:

- maintain processing records (controller/processors);
- support project managers in the application of data protection requirements;
- generate contact forms to exercise people's rights and manage how they are processed;
- maintain a register of processors;
- manage notifications of incidents;
- more generally, enable compliance with legislation within the Elior Group in accordance with the principle of accountability.

However, it is the responsibility of:

- project managers (IS controller and business needs manager) to inform any new data processing within this environment and the personal data ambassadors to support and approve the information provided;
- personal data ambassadors to ensure that requests to exercise rights are properly handled with the support of IS controllers and business needs managers.

C. Personal Data Steering Committee (PD SC)

Led by the DPO and under the chairmanship of the Group Chief Compliance Officer, the Personal Data Steering Committee is the decision-making body.

In particular, it has the following responsibilities relating to the protection of personal data within the Elior Group:

- approving the policy and its changes;
- drawing up the annual review of actions;
- taking note of the level of compliance;
- approving and arbitrating the priority of actions.

In addition to the Group team, the PD SC comprises the following members:

- the Group Information Systems Director;
- the Group General Counsel;
- the Group Internal Audit Director;
- the Group Insurance and Risk Prevention Director;
- the Operations Information Systems Directors;
- The general counsels of operations.

A compendium of the decisions of the PD SC will be formalised by the DPO at the end of the committee meetings. Reports will be accessible to all stakeholders.

The PD SC meets each year. It may meet extraordinarily on the occasion of an event deemed significant, on the proposal of the DPO (major incident, major arbitration, oversight of the authorities, etc.).

D. Working Group on the Protection of Personal Data (WG)

Led by the IT Security Compliance Manager and the Group Senior Legal Counsel under the chairmanship of the DPO, the personal data operational committee is the body for planning and monitoring recommendations issued by the PD SC.

In addition to the Group team, there are also personal data ambassadors from the (collective catering, concession catering and services) zones and, depending on the opportunity, personal data ambassadors internationally.

The PD SC meets as and when appropriate.

E. Crossover coordination

The IT Security Compliance Manager is responsible for co-ordinating work on the protection of personal data in France and internationally. He/she is also responsible for identifying and disseminating the associated best practices within the Elior Group.

4. Our obligations

This section describes the various personal data protection obligations of the Elior Group.

A. Liability and processing inventories

The General Data Protection Regulation introduces the principle of accountability in connection with data processing. Since its entry into force, the Elior Group must be able to demonstrate that it complies with the regulations; this involves in particular carrying out an inventory of the data processing implemented.

Thus, two types of registers must be maintained within the Elior Group; the first concerns processing for which any Elior Group entity is responsible, the second concerns processing for which any Elior Group entity acts as processor.

For each processing task for which Elior Group acts as a controller, the following information must be included in the register:

- the identity of the controller and processors;
- the identity and contact details of the IS controllers and business needs managers;
- the purpose (the objective pursued by the collection and processing of data);
- the legal basis for processing;
- the list of data collected, their retention period and the persons concerned;
- the categories of persons having access to the data (administrator, human resources, processors, etc.);
- the presence of transfers to a third country;
- the way in which people are informed;
- the security measures put in place;

- possibly, the results of the DPIA.

For each processing task for which Elior Group acts as a processor, the following information must be included in the register:

- the name and contact details of each client on whose behalf the data are processed;
- the name and contact details of each processor, where appropriate;
- the categories of processing tasks carried out on behalf of each customer;
- the transfers of data outside the EU on behalf of the client;
- where possible, a general description of the technical and organizational security measures implemented.

It is the responsibility of the IS controllers and business needs managers to complete this register using their DCP ambassadors.

B. Transparency and loyalty

Transparency

It is the duty of the Elior Group and its teams to be clear and transparent about the processing of personal data. Any data collected must not be used in a manner and for a purpose that would not be reasonably expected and anticipated with regard to the intended pursued.

Therefore, before any personal data are collected, it is necessary to communicate in clear and simple language on:

- who we are;
- what personal data are being collected and from which source;
- the operations that will be carried out with this personal data and the legal basis;
- whether the personal data are or will be shared with other recipients;
- the retention period for personal data;
- whether the personal data will be transferred outside the European Economic Area;
- the rights guaranteed to persons relating to the processing of personal data.

Lawfulness of the processing

In order for the processing of personal data to be lawful, there must be legitimate reasons or justified legal obligations or the consent of the data subject must have been obtained. Thus, prior to any processing of personal data, in addition to informing individuals, it is necessary to ensure that this processing is based on one of the following:

- **Legal obligation** - the processing is necessary for compliance with a legal obligation to which the controller is subject (national law or European Union law); for example, the communication of employee remuneration data to the social security and tax authorities.

- **Contractual requirement** : 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;
  This situation must only cover the services essential to the performance of the contract and in particular exclude any commercial canvassing; for example, the collection of the contact details of a guest for the publication and sending of invoices or the processing of employee data for the implementation of the payroll.

- **Legitimate Interests** - 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 or fundamental rights and freedoms of the data subject which require protection of personal data. The legitimate interest of the controller must then be systematically weighed against the fundamental rights and freedoms of the persons concerned; for example, the communication of information relating to corruption to an authority outside the European Union or the analysis of Internet traffic to prevent access to malicious systems for the purpose of IT network security.

- **Vital interests** - processing is necessary in order to protect the vital interests of the data subject or of another natural person; for example, collecting a personal telephone number for sending alert text messages in the event of serious events in the workplace or collecting data relating to a specific diet to prevent any risk to a person's health.

- **Public interest** - this legal basis concerns a situation in which official authority or a mission of public interest is vested in the controller, for which processing is necessary. Should this situation arise, this legal basis must be used on a case-by-case basis after approval by a personal data ambassador.

- **Consent to the collection** - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    - His/her consent must be free (actual choice, without negative consequences), specific (specific consent for each purpose), informed (presence, at the time of expression of consent, of appropriate and sufficient information) and unambiguous (opt-in logic, no ambiguity and absence of consent by default or linked to inaction);
    - the collection of consent must be demonstrable (e.g. checkbox, form to be completed, systematic procedures or mechanisms) and give the person the possibility to withdraw it.

Data minimization

In addition, any information collected and recorded must be relevant and strictly necessary for the intended purpose. Measures must therefore be taken to reduce to a minimum the volume of personal data collected and to ensure that they are adequate for the purposes of the processing.

C. Maintain accurate data and retain them for a limited period

Possessing incorrect or inaccurate information about a person may be a source of harm. For example, a person could be excluded from advantages or benefits related to their status. Particular care should therefore be taken when a decision is taken based on personal data.

Accuracy of data

Elior Group employees must ensure that the information held is accurate. This is guaranteed by the implementation of the following mechanisms:

- verifying the accuracy of the information at the time of collection where possible;
- where possible, giving data subjects the opportunity to update their data;
- periodically reviewing retained personal data to ensure that they are still up to date;
- correcting or deleting any inaccurate data.

Risks inherent in free text fields (FTF)

Special precautions must be taken regarding the text fields and comment areas. These free text fields are useful for following up a file or personalising a relationship. While it is not prohibited to use them, awareness-raising actions and management rules must govern their use to prevent the comments entered from infringing the rights of the persons concerned.

Some comments may prove to be derogatory, discriminatory or even offensive, or may reveal so-called sensitive data, such as health data. Comments must therefore be appropriate, objective and respectful.

The best precaution is to keep in mind that the people concerned (customers, guests, employees, etc.) can, at any time and upon simple request, access the content of these text areas by exercising their right of access.

Retention period

Personal data cannot be kept indefinitely, so a retention period must be set in accordance with the purpose which led to these data being collected. Once this objective has been achieved, these data must, as the case may be, be archived, deleted or anonymized (notably to produce statistics).

It is important to note that in the legitimate interest of the Elior Group and to defend its interests, these data may nevertheless be retained for longer periods, justified by a specific context, in the context of litigation, for example, and in all cases after informing the DPO.

D. Ensuring data security

Data security is a key issue for Elior Group. Failure to ensure the security of data over their entire life cycle, from collection to destruction, may lead to significant harm for individuals. Increased vigilance must be given to the security of external providers when they are stakeholders in the processing of personal data.

There are many ways to protect personal data, whether they are stored in electronic or paper form. In order to support its teams, the Elior Group offers them a state-of-the-art body of documents, which must be applied:

- a security policy for information systems and associated directives detailing the requirements applicable to Elior Group information systems;

- security requirements that are a prerequisite to any contract with an IT service provider.

The recommendations presented below must be adapted on a case-by-case basis and according to the risks incurred by data processing on the freedoms and privacy of the persons concerned:

- applications must be protected by authentication systems (username and password) in accordance with the information security policy;
- access to personal data is only authorised for persons accredited to have access to the data in question, this is "the right to know ".
- regardless of the type of physical, digital or paper medium, the latter must be secured. Particular care must be taken with regard to mobile equipment, which must not be left unattended or protected.

If you have any questions, contact the Elior Group Information Systems Security Manager.

E. Processing and transfer of personal data

In the event of a transfer of personal data, Elior Group must first ensure that it is legally possible and secure. The transfer of personal data must be interpreted broadly; for example, it may be:

- data transfers between legal entities within the Elior Group;
- outsourced administration or maintenance of an IT resource;
- hosting a service in the cloud.

The processor's obligations

In accordance with the GDPR, the processor is required to support the controller in its ongoing compliance process. The controller is responsible for ensuring that the processor performs this task. The processor must be required to ensure:

- **transparency** - made possible by the drafting of a legal act (i) clearly defining the obligations of each of the parties, (ii) specifying that the processor is acting solely on the instructions of the controller. This transparency is also guaranteed by maintaining an up-to-date register of activities carried out on behalf of the controller and by making all the information required available to demonstrate compliance with these obligations;
- **advice and assistance** - the processor must support the controller in determining whatever data are strictly necessary, in processing requests to exercise rights and more generally for all its obligations;
- **security** - the processor must ensure that its employees are subject to a confidentiality obligation and must take all measures to ensure a level of security appropriate to the risks and data retention for the precise duration expected;
- **notification** - the processor must notify the controller of any data breach within a reasonable period of time (ideally 24 or 36 hours).

Elior Group and its teams undertake to ensure compliance with these requirements each time processors are used and when Elior Group acts as a processor.

When the Elior Group acts as a controller and uses one or more processors, the latter must comply with the Elior Group's personal data protection requirements. Data transfer to processors must be done in a secure manner. The Elior Group is responsible for ensuring that its processors have put in place adequate measures to ensure the security of personal data.

Legal departments must be systematically consulted in order to verify that any contract provides for the required obligations regarding the protection of personal data.

Special case of transfers outside the European Economic Area (EEA)

The transfer of personal data outside the EEA must be supported by appropriate mechanisms, for example:

- the signing of standard contractual clauses approved by the European Commission ;
- the drafting of binding corporate rules: "Controller" BCR or "Processor" BCR;
- the signing of specific commitments (e.g. Privacy Shield) for organizations based outside the EEA.

F. Exercise of rights

Elior Group ensures that the persons concerned are able to fully enjoy their rights, in particular:

- access their personal data;
- request rectification of their personal data ;
- request the portability of their personal data in a structured format;
- object to a decision based exclusively on automated processing;
- request the erasure of personal data;
- request limitations on the processing of personal data;
- object to the processing of personal data.

G. Privacy by design

It is simpler and cheaper to take privacy and security considerations into account as early as possible in projects. This is why, from the start of a new project, the project manager is responsible for taking into account the issue of personal data protection, and for ensuring respect for the privacy of the persons concerned, whether when setting up a new service/product or when modifying it.

This means, in particular, that for any new project, the project manager must:

- identify any personal data that may be present;
- if applicable:
    - enter this project into the personal data protection management tool and follow the instructions,
    - identify the main risks associated with personal data that may arise in the context of a particular project, in particular legal, reputational and personal risks,
    - for processing high-risk data, carry out a data protection impact assessment ("DPIA"). These processing tasks concern in particular the use of large-scale data, the use of new technologies, the processing of sensitive data, the systematic monitoring or the implementation of processing aimed at automated decision-making and profiling. The European Data Protection Committee refers on its site, country by country, to the list of processing tasks for which a DPIA is mandatory,
    - ensuring compliance with Group policy,
    - ensuring the implementation and monitoring of organisational and technical protection mechanisms.

In case support or clarification is needed, the project manager can turn to his personal data ambassadors.

H. Communication and awareness-raising

Each year, depending on the issues identified and the observations relating to Elior Group compliance, a communication and awareness-raising plan is initiated by the Group team with the support of the personal data ambassadors. The aim of this approach must be to establish a culture of personal data protection within the Elior Group.

The teams are invited to contribute to improving the policy and associated processes.

I. Special categories of processing and personal data

Sensitive personal data or equivalent

This refers to information that reveals the racial or ethnic origins, political, philosophical or religious opinions, trade union membership, health or sexual life of a natural person. Information on infringements or convictions must also be considered to be in this category.

It is recommended within the Elior Group to not collect or use these data due to the high risks relating to personal privacy, except in certain specific cases:

- if the data subject has given his or her express consent (written, clear and explicit);
- if these data are necessary for medical purposes or for research into health matters;
- if their use is authorised by the personal data protection authority.

As these cases may vary according to the national law of the country, it is therefore necessary to contact the personal data ambassadors or the Group GDPR team for this type of issue. A DPIA must always be performed.

Personal data and image rights relating to children

Children deserve specific protection with regard to their personal data because they may be less aware of the risks, consequences or guarantees that need to be provided and their rights relating to the processing of personal data.

In the context of the information society services, the processing of personal data relating to a child is lawful when the child is at least 16 years of age. Where the child is under the age of 16, this processing is only lawful if, and to the extent that, consent is given or authorised by the person having parental responsibility over the child. Member States may by law provide for a lower age for these purposes provided that this lower age is not below 13 years. Do not hesitate to contact the personal data ambassador to identify the age threshold based on the processing envisaged.

A DPIA must always be performed before these processing tasks are implemented.

Marketing operations

Marketing operations must respect the choices and rights of the people concerned. During marketing operations, particularly by electronic means, it must be ensured that:

- data subjects have given their express consent (for BtoC relationships);
- they have not exercised their right to object to prospecting;
- messages offer the possibility of easy opt-out;
- no recipient can see the names and contact details of another recipient.

J. Data breaches

Despite the application of high standards to ensure data security, Elior Group cannot fully protect itself against the risk of data breaches, which may be defined by:

- A breach of confidentiality, i.e. a data leak (e.g. loss of USB key containing customer files);
- a breach of integrity, i.e. an unplanned modification (e.g. an undesired modification of the database which automatically indicates to the authorities who is the beneficiary of a company vehicle);
- a breach of availability, i.e. destruction of data (e.g. malware encrypting a database).

The source of these violations can be either external (e.g. attack on an Elior Group resource or a service provider exposed to the Internet) or internal. It may also be intentional or accidental (e.g. screen not protected by a confidentiality filter on public transport).

It is everyone's responsibility to be vigilant and to notify any data breach without delay to the Group GDPR team. In the event of an actual or suspected breach of security, immediate action must be taken to limit the effects and damage. In the most serious cases, Elior Group must inform the competent data protection authority and provide it with an action plan enabling it to mitigate the impacts of the breach within 72 hours and, in some cases, also inform the persons concerned.

K. Control and relationship with the data protection authorities

Potential impacts of not taking personal data protection into account

Violations of personal data protection legislation may have serious consequences, including:

- financial penalties of up to 4% of Elior Group's total turnover;
- requests for compensation from persons affected by the breach of privacy;
- compliance under penalty, limitation of processing or suspension of data flows;
- damage to the reputation and image of the Elior Group.

Power of data protection authorities

Elior Group is currently drafting *Binding Corporate Rules*. The purpose of these BCRs is to demonstrate compliance with a similar level of data protection regardless of the location of the legal entity that is a subsidiary of the Elior Group and to authorise the transfer of personal data within the Elior Group.

The personal data protection authority has the power to monitor compliance with the General Data Protection Regulation via physical or remote controls and may in particular:

- obtain a copy of the maximum amount of technical and legal information, to assess the conditions under which the processing of personal data is carried out;

- request the communication of all documents necessary for the performance of its mission;
- access computer programs and data, and request transcription;
- request copies of contracts (e.g. file rental contracts, IT outsourcing contracts), forms, paper files, databases, etc.
- carry out vulnerability scans and security audits remotely and check the presence of legal information notices.

In France, Article 51 of Law no. 78-17 of 6 January 1978, as amended, relating to information technology, files and freedoms, known as the "Data Protection Act", provides that any obstruction of CNIL's action is punishable by one year's imprisonment and a €15,000 fine. The Personal Data Protection Authority is obstructed in the event of:

- opposition to the exercise of the missions entrusted to authorised members or agents when the visit has been authorised by the magistrate for custody and release (juge des libertés et de la détention);
- refusal to disclose, concealment or destruction of the information and documents required for the audit;
- provision of information that does not comply with the content of the records as it was at the time the request by the personal data protection authority was made or the presentation of content in a form that is not directly accessible.

How to proceed:

It is recommended that the Group team be contacted without delay and full co-operation with the authorities after verifying the identity of the persons (warrant and professional identity card).

The Group team is the only entity authorised to communicate with data protection authorities (e.g. prior procedure, request for information, response to referrals, etc.). It must therefore be informed of any request from the authorities without delay.

5. Additional information

If you have any questions about this policy or if you would like more information on any of the topics covered in it, please contact the Group team via the following email address: gdpr-contact@eliorgroup.com.