

2018-03-28


PERSONAL DATA PROTECTION POLICY

SIACI SAINT HONORÉ

S2H

Season, 39 rue Mstislav Rostropovitch - 75815 Paris cedex 17 - France

Tel: +33 (0)1 4420 9999 Fax: +33 (0)1 4420 9500



GENERAL INFORMATION

Date	2018/03/28
Title	Personal Data Protection Policy (PDPP)
Issuing division	Risk and Compliance Division
Approved by	Risk and Compliance Division & Legal Division
Person(s) in charge of document	Samanta Le Pont
Dissemination	Public information This document is disseminated among all S2H internal departments and may be disseminated as part of business relations (clients, risk carriers, sub-contractors).
Versions	1 st version: 2018/03/28

CONTENTS

1. BACKGROUND	4
1.1 Regulatory background	4
1.2 Internal background	4
2. AREA OF APPLICATION	5
2.1 Definitions	5
2.2 Scope of the Policy	5
3. PURPOSE OF THE POLICY	6
4. DETAILED ORGANISATION REGARDING PERSONAL DATA PROTECTION	6
4.1 Organisation regarding personal data protection	6
4.2 The roles and responsibilities of the organisation regarding personal data protection	6
a. <i>The DPO</i>	6
b. <i>Data Protection Correspondents (DPC)</i>	8
c. <i>IT Risk Managers (ITRM)</i>	9
d. <i>The Risk and Compliance Division</i>	9
e. <i>The Legal Division</i>	9
f. <i>The Information Systems Division</i>	9
4.3 Steering and monitoring systems	9
5. THE CORE PRINCIPLES OF PERSONAL DATA PROTECTION	10
5.1 Collection	10
5.2 Data processing declarations	11
5.3 Privacy Impact Assessment	12
5.4 Processing security	12
5.5 The specific case of the NIR identification number and data on health	13
5.6 Data subjects’ rights	14
5.7 Personal data transfers	15
5.8 Processors	15
5.9 Supervision	16
5.10 Data protection as early as the project design phase and at the highest level of protection	16
5.11 Management of data breaches	16
5.12 The fate of data once the service is completed	17
6. PERIODICAL COMPLIANCE AUDITS	17
APPENDIX 1	18
APPENDIX 2	21
APPENDIX 3	22
APPENDIX 4	23

GLOSSARY

CNIL	Commission Nationale de l'Informatique et des Libertés, the French Data Protection Agency.
Controller	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 concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
DPO	Data Protection Officer
GDPR	General Data Protection Regulation. As this is a European Regulation, it is directly applicable in the legal system of European Union Member States.
NIR	<i>Numéro d'Inscription au Répertoire national</i> , a natural person's French social security identification number.
Personal data	Any information relating to an identified or identifiable natural person ('data subject').
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Sensitive data	<p>Under the GDPR, sensitive data concerns:</p> <ul style="list-style-type: none"> - racial or ethnic origin; - political opinions, religious or philosophical beliefs or trade-union membership; - health, sex life or sexual orientation; - genetic data; - biometric data for the purpose of uniquely identifying a natural person. <p>The Siaci Saint Honoré Group has decided to consider a person's NIR (French social security identification number) as sensitive data and to protect it accordingly.</p>
User	Any person who handles computerised or non-computerised personal data and any person who conducts automated or non-automated processing actions of this type of data, regardless of the status of the User.

1. **BACKGROUND**

1.1 Regulatory background

In France, legislation regulating personal data* protection originates from the “*Loi Informatique et Libertés*” (French Data Protection Act) dated 6 January 1978¹ which has since been regularly amended. Personal data protection is a key issue on both a European level, with the Directive dated 24 October 1995², and a national level as this Directive was transposed into French legislation by the Law dated 6 August 2004³ (which amended the French Data Protection Act).

More recently, the General Data Protection Regulation (hereafter “GDPR”), which entered into force on 24 May 2016 and becomes applicable on 25 May 2018 in all European Union Member States, replaces the European Data Protection Directive (Directive 95/46/EC).

Today, people are very careful with their personal data and with data protection in order to preserve confidentiality (in particular for financial or health-related data). They expect their privacy to be respected and that the companies to which they entrust their data are able to protect them.

This is why Siaci Saint Honoré (hereafter “the Group”) is working to ensure the security of data entrusted to it. Going beyond regulatory compliance, this concerns the very essence of its businesses.

Exposure to the following risks may be possible due to shortcomings in protection procedures:

- Risks of damage to image and reputation;
- Legal risks, sanctions by the market or the regulator, accountability in the event of identity theft;
- Discrediting of the company vis-à-vis its clients or employees;
- A loss of business and the repercussions on profit and market share losses.

There may also be a considerable impact in the event of an administrative fine imposed by a regulatory authority such as the Commission de l’Informatique et des Libertés (French Data Protection Agency) (hereafter “CNIL”) which for companies may represent up to 4% of total worldwide annual turnover of the preceding financial year⁴.

1.2 Internal background

The Siaci Saint Honoré Group is a leading provider in France in insurance consulting and brokerage services specializing in health & life and property & casualty risks for companies.

In certain situations, the Group may act as a controller* and in others as a processor*. Aware of the challenges raised by these different roles, the Siaci Saint Honoré Group has drawn up this Personal Data Protection Policy (hereafter “PDPP”) to cover all the principles applicable to personal data collected and processed as part of its business.

¹ French Law No. 78-17 dated 6 January 1978 on IT, files and freedoms.

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³ French Law No. 2004-801 dated 6 August 2004 on the protection of individuals with regard to the processing of personal data, amending the Law No. 78-17 dated 6 January 1978 on IT, files and freedoms.

⁴ Article 83 GDPR.

2. AREA OF APPLICATION

2.1 Definitions

- *Personal data*

According to the GDPR, personal data means “any information relating to an identified or identifiable natural person ('data subject')”⁵.

As part of its business, in particular for health and life insurance but also in the event of personal injury, the Group must collect and handle personal data such as first and last names, age and address, and also so-called “sensitive” data.

- *Sensitive data*

Under the GDPR, sensitive data* concerns:

- racial or ethnic origin;
- political opinions, religious or philosophical beliefs or trade-union membership;
- health⁶, sex life or sexual orientation;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person.

As part of its business, the Group must also process French social security identification numbers (*Numéro d'Identification au Registre national*) (hereafter “NIR”). While this form of identification does not come under the definition of sensitive data by the French Data Protection Agency (hereafter “CNIL”), Siaci Saint Honoré has opted to apply the same rules to NIRs as to sensitive data.

2.2 Scope of the Policy

This PDPP is applicable to all Users* of personal data within the Group. A User may be any person who handles computerised or non-computerised personal data and any person who conducts automated or non-automated processing actions of this type of data, regardless of the status of the User.

On a contractual basis, this PDPP is therefore applicable to partners and service providers and to all processors who may collect and/or process personal data acting on behalf of the Group and on its instructions.

In addition, any use of personal data is conducted within a professional and responsible framework, i.e. within the exclusive scope of the User’s assignments and functions as defined by the Group. The controller’s instructions must be followed and compliance must be supervised⁷. This means that the User is responsible for the use made of the Group’s resources in the exercise of his/her duties.

In this respect, the Group **Information System Security Policy** (hereafter “ISSP”) states that any new employee in the Group must acquaint themselves with the *Charter for the use of IT resources and Internet services*.

The Groupe undertakes to process data in a confidential manner. To achieve this, access to the information system is subject to authorisation and is monitored.

⁵ Article 4, 1° GDPR.

⁶ Art. 4, 15° GDPR: data concerning health means “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”.

⁷ Art. 32, 4° GDPR.

According to the Group ISSP, four (4) types of directives have been implemented concerning the identification, authentication, authorisation and responsibility of managing the rights granted to profiles. Compliance with these principles is a means of granting users access solely to the rights they really require in the exercise of their duties in order to avoid any unnecessary access and to limit the consequences of a failure of the authentication systems.

3. PURPOSE OF THE POLICY

Due to its international presence, the Group must comply with the French Data Protection Act, the GDPR and European Directives (such as the Directive on the cross-border exchange of information⁸), and also with applicable local legislations.

The purpose of the PDPP is therefore to set an overall and common framework for the protection of personal data entrusted to the Group, while preserving the specific features of each entity, in relation to risk exposure and applicable legislation and situations.

The ISSP also provides that the Group must incorporate requirements related to:

- The new GDPR;
- The hosting of health-related data;
- Defence-related classified information.

4. DETAILED ORGANISATION REGARDING PERSONAL DATA PROTECTION

4.1 Organisation regarding personal data protection

The GDPR requires the Siaci Saint Honoré Group to appoint a Data Protection Officer (DPO), given the considerable volume of data it processes, and in particular sensitive data⁹.

In order to ensure the best possible management of compliance by all its companies with regard to the regulation applicable to personal data, the Group has decided to appoint a DPO and in addition a network of “Data Protection Correspondents” (hereafter “DPC”) and of IT Risk Managers (hereafter “ITRM”) in order to ensure that data protection is dynamic and effective across the Group.

A “Personal Data Committee” has also been created.

4.2 The roles and responsibilities of the organisation regarding personal data protection

a. The DPO

The Group appointed Samanta Le Pont, Director of the Risk and Compliance Division as Data Protection Correspondent (CIL – *Correspondant Informatique et Libertés*):

- For S2H, MSH International, Assurance et Réassurances Techniques, GA Prévoyance Conseils and S2H Consulting: effective from 13 July 2017 (Reference CIL 111540).
- For Cap Marine Assurance et Réassurance: effective from 19 August 2017 (Reference CIL 171753).
- For MyP.

⁸ Directive 2011/82/EU of the European Parliament and of the Council of 25 October 2011 facilitating the cross-border exchange of information on road safety related traffic offences.

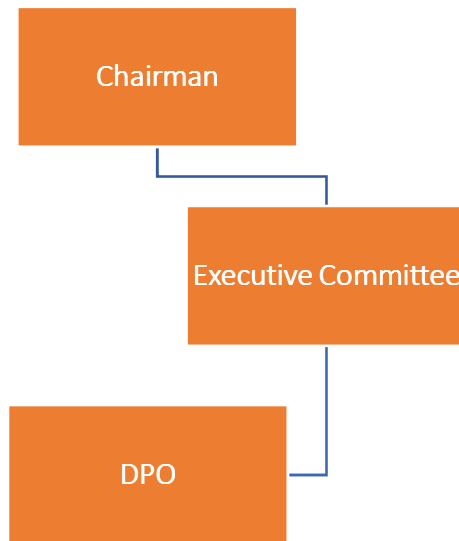
⁹ Art. 37, 1° c) GDPR.

The CNIL stated in letters to the CILs currently in the role that they do not have to become DPOs. This choice is made by the Controller* and must consider several criteria such as:

- The absence of conflicts of interest;
- The professional skills required for the performance of the DPO’s duties (legal and technical expertise, knowledge of the insurance industry, etc.);
- Impartiality
- The personal qualities which are essential for the exercise of such duties (probity, loyalty, etc.).

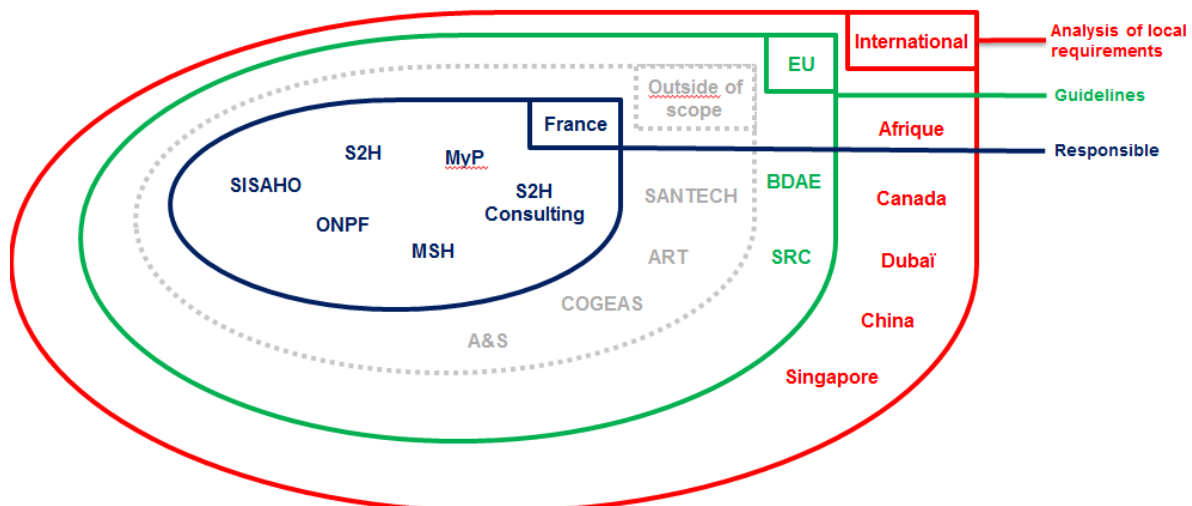
After considering these different criteria, the Group has opted to appoint the current CIL as DPO.

The DPO reports to the General Secretary, who is a member of the Siaci Saint Honoré Group’s Executive Committee and who reports directly to the Chairman.



The DPO plays a central role.

The scope defined for the DPO’s involvement is as follows:



The DPO keeps a register of processing in which all processing actions conducted by the Group's subsidiaries and entities in France are listed.

While the GDPR does not state any requirement with regard to a DPO register, the Group DPO will continue to keep this register with a view to monitoring processing and accountability (proof of compliance).

The DPO disseminates guides and recommendations to subsidiaries outside of France to ensure local registers are properly kept.

The DPO must be consulted prior to the implementation of any processing ("New Project" form in APPENDIX 1). The DPO ensures compliance with the applicable data protection legislation in the European Economic Area (EEA). His/her opinions and recommendations must be sought before any new project is rolled out.

It is the DPO's role to discuss data protection with the various divisions (Information Systems Division, Legal Division, Risk and Compliance Division, etc.) and with the various Data Protection Correspondents (DPC) and IT Risk Managers (ITRM) appointed within each business line or department in the Group's entities in France.

The DPO issues instructions to compliance officers in the Group entities outside of France.

The DPO's role includes in particular:

- Leading and coordinating the personal data protection procedure;
- Ensuring compliance with the GDPR and with internal rules;
- Interacting and cooperating with the supervisory authority.

It should be noted that the DPO is not personally accountable in the event of the Group's non-compliance with GDPR.

The DPO analyses processing compliance in line with data protection regulations. This analysis focuses in particular on: the purpose and proportionality of the processing, the relevance of data in line with the purpose, the length of time data is stored, data recipients, the management of relations with processors, security measures, notification of data subjects and the terms of exercising their rights and, where necessary, the management of cross-border data flows.

The DPO must also notify the Group of any breaches observed and advise on the response required to remedy any such issues.

The DPO and his/her team conduct awareness-raising initiatives for Siaci Saint Honoré Group employees and where necessary provide training through ad hoc sessions.

For the performance of all these duties, the DPO must ensure that his/her skills are maintained by keeping abreast of the latest personal data protection developments. He/she must also regularly attend training courses or conferences on this issue.

b. Data Protection Correspondents (DPC)

DPCs are appointed within each business line and are tasked with being the data protection contacts for their respective scope of activity. They are the DPO's point of contact for their area of responsibility. They may be contacted by operational employees with questions regarding data protection.

In addition to their operational activities, their main duties are to:

- organise bottom-up feedback on all new data processing projects to bring about discussions with the DPO and the Information Systems Division;

- raise awareness of personal data protection within their Divisions;
- take part in projects concerning personal data protection;
- ensure continuous alert thresholds as regards data protection compliance within their Division.

c. IT Risk Managers (ITRM)

ITRMs ensure compliance with personal data protection obligations on a day-to-day basis within the Information System (IS). They:

- manage the personal data protection approach in the Information Systems (IS);
- instigate bottom-up and top-down feedback with the DPO;
- take part in regular discussions with Data Protection Correspondents (DPCs).

d. The Risk and Compliance Division

The Risk and Compliance Division (hereafter “RCD”) assists the DPO in the performance of his/her duties and provides expertise on risk analysis and compliance. It takes part in updating internal documentation (risk mapping, internal control policy, internal control plan, etc.).

The RCD also contributes to privacy impact assessments with operational employees and the DPO.

e. The Legal Division

The Legal Division (hereafter “LD”) provides legal support and expertise for the performance of the DPO’s duties. In particular, it takes part in updating contractualisation and pre-contractualisation procedures and the drafting of standard contractual clauses.

The LD also monitors regulatory and legislative developments in France regarding data protection.

f. The Information Systems Division

The Information Systems Division (hereafter “ISD”) assists the DPO in the performance of his/her duties and provides expertise on the securing of applications and architecture principles.

The main roles of the ISD as regards personal data protection are described in the Group ISSP.

As stated in the **Group ISSP**, different roles and responsibilities must be clearly defined. The organisation memorandum, drafted jointly with the ISD, sets out the organisation of information system security within the Group and defines the company’s roles and responsibilities with regard to information system security management.

4.3 Steering and monitoring systems

The Group has created a Personal Data Committee which:

- steers the progress of project work;
- approves structuring options and expected arbitration;
- approves the project’s key deliverables;
- coordinates the various project stakeholders throughout the project;
- sets the project’s objectives and direction.

This Committee is comprised of:

- The Secretary General;
- The Information Systems Division;
- The Human Resources Division;
- The Communications Division;
- The Legal Division;
- The MSH General Management Division;
- The Risk and Compliance Division;
- The Life Development Division;
- The Property & Casualty and Marine Division.

The Committee meets at least twice a year and has the option of convening an emergency Committee meeting in the event of an issue that must be resolved swiftly.

The Siaci Saint Honoré Group promotes a data protection culture among all employees.

The Group ensures that all employees are aware of and comply with the principles applicable to personal data protection in the implementation of personal and sensitive data collection and processing.

Training is also provided to all employees and the Group publishes regular updates on its Intranet on issues related to personal data protection. The dissemination of newsletters has been stepped up over the period from January 2018 to May 2018 and will continue with a view to promoting the data protection culture within the Group.

According to the ISSP, employee training and awareness-raising initiatives concerning Information System Security (hereafter ISS) are a key ISS activity and must mitigate risk exposure.

The Information Systems and Human Resources Divisions ensure that:

- documents on security are disseminated and presented to all employees.
- employees enjoy and are aware of the means to access documentation in case of any doubt or questions.
- the necessary training courses are available.

5. THE CORE PRINCIPLES OF PERSONAL DATA PROTECTION

5.1 Collection

The Siaci Saint Honoré Group may only collect, process, store and record personal data within the Group in accordance with the instructions received by the User. This User must, as part of his/her duties, respect the core principles described below.

It is imperative that all Users, as part of their professional activity and/or duties within the Siaci Saint Honoré Group, comply with the principles of **loyalty, lawfulness and legality** required by the applicable personal data protection regulations when collecting personal data.

To ensure that data collection is loyal, lawful and legal, the data subject concerned by the collection and processing of data belonging to him/her must receive information in a concise, transparent, intelligible and easily accessible form, using clear and plain language from the person who collects such data¹⁰.

¹⁰ Art. 12 GDPR and Art. 90 of the French Order dated 20 October 2005.

For **direct collection**¹¹ (e.g.: registration form), the following information must be provided at the time of collection:

- The identity and contact details of the controller and, where necessary, of the controller's representative;
- The DPO's contact details;
- The purpose of the processing;
- The legal basis of the processing (APPENDIX 2). If the processing is based on the controller's legitimate interest, it is necessary to specify these grounds. In this case, it is also necessary to inform the data subject that they may withdraw their consent at any time, without prejudice to the lawfulness of the processing based on the consent given prior to its withdrawal;
- The data recipient(s) or category(ies) of recipient(s);
- The intention of transferring data to a third country or an international organisation, and the existence or absence of an adequacy decision issued by the Commission or the reference to appropriate or adapted safeguards and the means of obtaining a copy or the location in which they are made available;
- The length of time the data will be stored, or if this is not possible the criteria used to determine the timeframe;
- Access, rectification, suppression, restriction, opposition and portability rights;
- The option of organising instructions upon the data subject's death;
- The right to file a complaint with a supervisory authority;
- For each data item, the mandatory or optional nature and the potential consequences of non-provision of such data (if the requirement to provide data is pursuant to regulations or contracts or if it conditions the signature of a contract);
- The existence of an automated decision, including profiling and information concerning the underlying approach and the planned importance and consequences of the processing for the data subject.

For **indirect collection**¹² (e.g.: the purchase of a prospecting file), it is necessary to provide all the aforementioned information and in addition the source of the data. The data subject must be notified of this information:

- Within a maximum of one (1) month from the date on which the data was obtained;
- At the latest at the time of the first communication with the said data subject, if data must be used in order to communicate with the data subject;
- At the latest when data is disclosed for the first time, if data has to be disclosed to another recipient.

5.2 Data processing declarations

The GDPR repeals the CNIL's data processing pre-declaration scheme.

It is the Group's duty to conduct privacy impact assessments on data subjects in order to measure the risk raised by any new processing operations which are envisaged. If, following this assessment, the risk proves high for the data subject's privacy, the Group must consult the CNIL to request an opinion or authorisation (only if technical and/or organisational measures taken are insufficient to mitigate the risk initially measured by the impact assessment).

¹¹ Art. 12 GDPR and Art. 32 of the French Data Protection Act.

¹² Art. 13 GDPR.

5.3 Privacy Impact Assessment

Now that pre-declarations are no longer required, the Siaci Saint Honoré Group assesses the risk levels of processing through criteria listed by the Article 29 Data Protection Working Party¹³:

- **Evaluation or scoring, including profiling and predicting:** this includes processing concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.
- **Automated decision-making with legal or similar significant effect:** processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person".
- **Systematic monitoring:** processing used to observe, monitor or control data subjects.
- **Sensitive data or data of a highly personal nature:** processing concerning categories of data as defined in articles 9 and 10 of the GDPR. It may also concern the processing of data considered as increasing the possible risk to the rights and freedoms (electronic communications, financial data, etc.)
- **Data processed on a large scale:** several factors must be considered when determining whether the processing is carried out on a large scale: the number of data subjects concerned, the volume of data and/or the range of different data items being processed, the duration, or permanence, of the data processing activity, the geographical extent of the processing activity.
- **Matching or combining datasets:** originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
- **Data concerning vulnerable data subjects:** this criterion considers the power imbalance between the data subjects and the data controller: children, employees, mentally ill persons, asylum seekers, or the elderly, patients, etc.
- **Innovative use or applying new technological or organisational solutions:** combining use of finger print and face recognition for improved physical access control.
- **When the processing in itself prevents data subjects from exercising a right or using a service or a contract:** this includes in particular processing operations that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

The Siaci Saint Honoré Group implements and shall implement a Privacy Impact Assessment in the event of at least two of these criteria being met. However, the DPO may decide that such an assessment must be conducted when only a single criterion is met and on grounds such as the presence of a sub-contracting chain or a transfer outside of the EU which are difficult to monitor.

5.4 Processing security

As stated in the **Group ISSP**, information system security is the status of protection against identified risks, resulting from all general and specific measures taken to ensure the confidentiality, availability and integrity of personal data.

¹³ The Article 29 Data Protection Working Party is an independent European advisory body on data protection and privacy. The Art. 29 WP will become the European Data Protection Board on 25 May 2018 (art. 68 and subsequent articles, GDPR).

The Siaci Saint Honoré Group undertakes to process personal data in such a way that guarantees appropriate data security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures to ensure a level of security appropriate to the risk¹⁴.

On this point, the **Group ISSP** sets out the general measures applicable to the Information System.

All processing of personal data conducted within the Siaci Saint Honoré Group must comply with protection rules¹⁵ governing:

- Physical security: measures aimed at limiting and controlling access to places where data is stored solely to authorised persons and preventing and protecting personal data against accidental or wilful attacks such as fire or water damage.
- Logical security: measures aimed at limiting and controlling access to Information Systems, including telecommunications, solely to authorised persons.

The **Group ISSP** states that the use of encryption techniques or procedures is not authorised without the approval of the ITRM. This document also sets out the security measures applicable to the Siaci Saint Honoré Information System.

The user is also informed of the existence of traceability implemented in order to secure the Group's business and Information System. All databases of the Siaci Saint Honoré Group have a solution used to log and trace access. This can determine which employee accesses the database, the operations conducted and the time this takes place.

The Group ISSP states that Directives on logging and the analysis of logs of network and telecom devices and on the analysis of system logs govern the traceability of data access.

5. 5 The specific case of the NIR identification number and data on health

For business related to health, pensions and life insurance, articles R115-1 and R115-2 of the French Social Security Code authorise the Group to collect and use the NIR Social Security identification number. However, this authorisation is only valid for processing conducted in the performance of the Group's health insurance, maternity, disability benefits and supplementary pensions activities.

The NIR is collected for all insured members who receive complementary healthcare insurance in order to create an automated link between the various local healthcare insurance offices (Caisses Primaires d'Assurance Maladie - CPAM) in France and the Group's departments. The aim is to structure and automate the healthcare reimbursement circuit with a view to making it more efficient and swift.

As regards health-related data, the Group has taken measures to preserve the confidentiality of such data and to comply with the recommendations of the Belorgey and AERAS conventions. The organisation and applicable principles are available internally in a document on medical confidentiality. In addition, the hosting company selected by the Group is certified "Hosting for Health-related Data".

¹⁴ Art. 32 GDPR and Art. 34 of the French Data Protection Act.

¹⁵ Art. 24 GDPR and Art. 34 of the French Data Protection Act.

5.6 Data subjects' rights

All natural persons who are subject to the Group's data processing enjoy various rights granted by national and European Union legislation. Compliance with these rights must be ensured and their implementation must be effective.

These natural persons enjoy a **right of access**¹⁶ and a **right to rectification**¹⁷ in order to obtain from the controller: the confirmation as to whether or not personal data concerning him or her are being processed or the rectification of inaccurate personal data concerning him or her. Data subjects may also provide instructions with regard to storing, deleting and disclosing their data after their death. This is known as the **option of organising the fate of personal data after the data subject's death**¹⁸.

All natural persons enjoy the **right to erasure**¹⁹ which is the right to obtain the erasure, under certain conditions, of personal data concerning them.

All natural persons also enjoy a right to **restrict**²⁰ and **oppose**²¹ the processing operation.

Persons also have the **right to data portability**²² which is the data subject's right to receive under certain conditions all data concerning them "in a structured, commonly used and machine-readable format"²³, to transmit those data to another controller.

Lastly, all natural persons have the right not to be subject to a decision based solely on automated processing, including **profiling**²⁴, which produces legal effects concerning him or her or similarly significantly affects him or her.

The controller must respond to requests by the data subject to exercise the rights afforded by the GDPR and the French Data Protection Act. The controller must provide the data subject with the information without undue delay and in any event **within one (1) month of receipt of the request**²⁵. This deadline may be extended by two (2) further months if the request is complex. In this case, the complexity of the request must be justified.

The Group has implemented a **Procedure for the administration of requests submitted by data subjects wishing to exercise their rights** as well as a dedicated **Manual**. In addition, the personal data management procedure sets out in detail the applicable terms and conditions as of the receipt of any request and the specific conditions applicable to a particular type of request. The Manual aims to set out quickly how the data subject's request may be answered fully within the legally required time.

All these documents are available internally from the Group DPO and all employees can access them via the personal Intranet. Regular dissemination operations are also held.

The DPO keeps and regularly updates a table of requests with a view to logging data subjects' requests for the exercise of their rights and the responses provided to them.

All requests submitted by data subjects must be sent to the Group DPO and processed by the DPO and his/her team members. The DPO can be contacted by email (at the following address:

¹⁶ Art. 15 GDPR and Art. 40 of the French Data Protection Act.

¹⁷ Art. 16 GDPR and Art. 40 of the French Data Protection Act.

¹⁸ Art. 32, I, 6° of the French Data Protection Act.

¹⁹ Art. 17, 1 GDPR and Art. 40 of the French Data Protection Act.

²⁰ Art. 18,1 GDPR.

²¹ Art. 21 GDPR and Art. 28 of the French Data Protection Act.

²² Art. 20,1 GDPR; Art. 48 of the French Law dated 16 October 2016 and Art. L 224-42-1 and subsequent articles of the French Code de la Consommation (Consumer Code).

²³ Art. 20 GDPR.

²⁴ Art. 22 GDPR.

²⁵ Art. 12,3° GDPR. The French Data Protection Act provided for a timeframe of two (2) months to respond.

dpo@s2hgroup.com). A transmission form for data subjects' requests to exercise their rights (APPENDIX 3 and APPENDIX 4) is made available to operational staff members to facilitate the transmission of requests. Once sent to the DPO, this form is used to provide an appropriate response to the data subject.

5.7 Personal data transfers

The Siaci Saint Honoré Group conducts its business over two types of geographic areas:

- Within the European Union;
- Outside of the European Union.

The transfer, import or export of personal data, outside of processing managed in the Group IS, may only be conducted following the prior, explicit and written instructions of the user's line manager and in compliance with the declarations or authorisations and notification of data subjects decided by the Group.

Transfers of personal data²⁶ are possible if:

- The country to which the transfer is made ensures an **adequate level of protection** acknowledged by the European Commission through an adequacy decision²⁷;
- The controller has provided **appropriate safeguards** and data subjects are informed of the transfer, and enforceable data subject rights and effective legal remedies are available²⁸. Appropriate safeguards may include the implementation of binding corporate rules²⁹ (or B.C.R.), standard clauses adopted by the European Commission, standard clauses adopted by a supervisory authority and approved by the European Commission or an approved certification mechanism. With the CNIL's authorisation, it is also possible to implement contractual clauses between the controller or the processor and the controller, the processor or the data recipient.

The Siaci Saint Honoré Group places significant importance on all personal data transfers outside of the European Union.

The ISSP states that data exchanges are governed by the Directives on the sending of IT media and data exchanges via electronic messaging.

The necessary authorisation requests have been submitted to the CNIL and are available from the Group DPO.

5.8 Processors

The GDPR pays special attention to the use of processors.

As part of the contracts signed with processors³⁰ tasked with processing personal data on its behalf (or of a Group entity), the Siaci Saint Honoré Group ensures that it is specified in the contract that:

- The processor is informed that data and files are subject to compliance with the applicable data protection legislation and come under privacy and professional confidentiality

²⁶ Art. 44, 45, 46, 47 and subsequent articles, GDPR.

²⁷ Art. 45 GDPR.

²⁸ Art. 46 GDPR.

²⁹ Art. 47 GDPR.

³⁰ Art. 4, 8° GDPR: processor "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

- requirements;
- And that the processor undertakes to implement all necessary procedures or measures to ensure the security and confidentiality of the data.

The Group guarantees that the processor provides sufficient safeguards to ensure the implementation of security and confidentiality measures and all processor contracts contain a clause on personal data protection setting out the responsibility of each party.

According to the **Group ISSP**, a service contract is signed between Siaci Saint Honoré and its hosting companies. This contract sets out the commitments of execution with regard to the requirements expressed by the project owners during the production launch. It describes the level of back-up, physical and logical security, the planned operating duties and the times of on-call duty, required availability and conservation measures.

5.9 Supervision

In addition to the compliance checks which may be conducted internally, the CNIL may have access, from 6 a.m. to 9 p.m., for the performance of its duties, to the sites and premises used to implement personal data processing³¹.

It may request the provision of all documents necessary for the performance of its assignment, regardless of the medium, and may take copies and access IT programs and data.

However, only a physician may request the provision of health-related data.

The Siaci Saint Honoré Group undertakes to cooperate with the CNIL in the event of checks.

5.10 Data protection as early as the project design phase and at the highest level of protection³²

In order to be able to ensure the Siaci Saint Honoré Group's compliance with data protection legislation, the DPO must be consulted as early as the initial phase of any project involving the processing of personal data.

Any user responsible for a new project falling within this scope must consult the DPO. To do so, the Group has created a "New Project" form (in APPENDIX 1) to allow the teams responsible for new projects to notify the DPO of the project in question and to receive his/her advice.

5.11 Management of data breaches

In the event of a security incident, Siaci Saint Honoré has implemented a Security Incident Management Procedure aimed at detecting, assessing and responding to a breach of data for example.

According to the **Group ISSP**, the incident management procedure enables teams to take effective action and pass on the information. The incident management system includes:

- Incident detection systems;

³¹ Art. 11-2° - f and Art. 44 of the French Data Protection Act.

³² Art. 25 GDPR.

- Reporting and processing following the detection of an incident up to crisis management;
- A consolidation of an information base;
- A monitoring system and a scoreboard.

The Group has also implemented a Business Continuity Plan in the event of critical downtime of any device or equipment. These solutions are described in the documents entitled “Business Continuity Plan” or “Disaster Recovery Plan” and include rules on triggering the plan, the actions to be conducted, the priorities, the persons to notify and their contact details.

5.12 The fate of data once the service is completed

As controller, the Siaci Saint Honoré Group regularly deletes data according to legal requirements.

As processor, the Siaci Saint Honoré Group undertakes to only process data on the documented instructions of the Client. According to the Client’s decision, the Group also undertakes to delete all data or to send data back to the Client at the end of the processing service and to destroy all existing copies.

6. PERIODICAL COMPLIANCE AUDITS

The Siaci Saint Honoré Group may conduct two types of audits:

- Internally, as part of the multi-year internal audit plan. The Siaci Saint Honoré Group internal audit is an independent and objective activity which provides the organisation with assurances on the extent to which its operations are controlled, advice to improve them and contributes to the creation of added value. The internal audit assists the Siaci Saint Honoré Group in reaching its objectives by assessing, through a systematic and methodological approach, its governance, risk management and control processes, while making proposals to heighten their effectiveness. The implementation of the internal audit is described in the **2017 S2H Group Internal Audit Charter**.
- With processors, as part of their contractual relations, in order to check that the principles applicable to personal data protection are correctly respected.

The Group provides the Client with all necessary information to demonstrate compliance with the obligations provided for by personal data protection legislation. The Siaci Saint Honoré Group also undertakes to allow the Client or an auditor instructed by the Client to conduct audits, and to contribute to these audits in accordance with the following conditions: one (1) audit per calendar year for which the request is submitted at least fifteen (15) days prior to the date on which the audit is conducted.

As regards information system audits, the **Group ISSP** states that they are planned and approved in order to minimize the risk of disrupting business processes. Access to system audit resources is protected in order to prevent any data being compromised or any inappropriate use.

APPENDIX 1

“NEW PROJECT” FORM

1. General details about the new project

- Title: _____
- Date of the new project: _____
- Person in charge: _____
- Department /Division: _____
- Date DPO notified: _____

2. Specific details about the new project:

- **Desired production launch date:** _____/_____/_____
- **Types of personal data concerned:**
 - Civil status / identity (last name, first name, email address, image):

 - Personal life (lifestyle, family situation): _____
 - Work life (CV, education, training): _____
 - Economic and financial details (income, tax situation): _____
 - Login data, cookies (IP address, logs): _____
 - Location data (travel, GPS data): _____
 - Other: _____
- **Presence of sensitive data?**
 - No
 - NIR = Social Security identification number
 - Health-related data: _____
 - Data on sex life or sexual orientation: _____
 - Data on criminal convictions: _____
 - Biometric data for the purpose of uniquely identifying a natural person:

 - Genetic data: _____
 - Data on trade-union membership: _____

Data on religious or philosophical beliefs: _____

Data revealing political opinions: _____

Data revealing racial or ethnic origin: _____

- **Type of collection:**

Directly from the data subject

Indirectly (use of another database, purchase of a file, etc.): _____

- **Type of data subject:**

Employees

Users

Visitors

Members

Clients (current)

Prospects (potential future clients)

Other: _____

- **Use of specific technology:**

Contactless device (RFID): _____

Anonymization mechanism: _____

Pseudonymization mechanism: _____

Smart card: _____

Geolocation: _____

Video protection: _____

Nanotechnologies: _____

Profiling: _____

Other: _____

- **Planned duration of data storage:**

1 month

2 months

3 months

For the period of the contractual relationship

Unlimited

Other: _____

- **Is permanent deletion possible following this timeframe?**

Yes: _____

No: _____

- **Is an archiving or automated deletion process planned?**

• Yes: _____

• No: _____

- **Data recipient(s):**

Other Division / Department of the S2H Group:

Service provider / Supplier: _____

Subsidiary / Other Group entity:

Data subjects: _____

Other: _____

- **Processing security:**

Physical access to the processing is protected

User authentication process in place

Connection logs

Processing conducted on a dedicated internal network (not connected to the Internet)

Other: _____

- **Transfers of data outside of the EU:**

Yes:

o To which country? _____

o Is the transfer secure? If so, how? _____

No

- **Data subject rights:**

- Are data subjects to be informed of the processing?

Yes. How? _____

No

- Will they be able to give their consent?

Yes. How? _____

No. Why? _____

- Is the exercise of data subjects' rights planned (access, rectification, portability, deletion, etc.)?

Yes. How? _____

No: _____

3. Divisions to be consulted:

Risk and Compliance Division _____ on ___/___/___

Legal Division: _____ on ___/___/___

Information Systems Division: _____ on ___/___/___

General Management: _____ on ___/___/___

APPENDIX 2

THE VARIOUS LEGAL FOUNDATIONS FOR PERSONAL DATA PROCESSING

Article 6, 1 of the GDPR sets out the various legal foundations which allow the controller to conduct personal data processing lawfully:

1. The specific and informed **consent** of the data subject;
2. 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 (e.g.: data required to take out an insurance policy);
3. Processing is necessary for **compliance with a legal obligation** to which the controller is subject (e.g.: obligations to combat money laundering and terrorist financing);
4. Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person (e.g.: the health of the data subject or of another person is compromised);
5. Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
6. Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party (assessment of the proportionality of interests between the controller and the data subject).

APPENDIX 3

TRANSMISSION FORM FOR DATA SUBJECTS' REQUESTS TO EXERCISE THEIR RIGHTS (INTERNAL)

Details of the person who has received the request:

- Request received on: ____/____/_____, at ____H____
- Request received by:
- Entity:
- Department:

Details on the data subject:

- Last name:
- First name:
- Postal address:
- Telephone:
- Email address:
- Other information stated:

Details on the request:

- ***Type of request*** (*tick the request submitted by the data subject – it is possible to tick more than one box – and state if the data subject has specified the request*)
 - Request for access:
 - Request for rectification:
 - Request for deletion / erasure:
 - Request for portability:
 - Request for restriction of the processing:
 - Request to oppose the processing:
 - Request to organise instructions following death:
- ***Request sent to the S2H Group DPO on:*** ____/____/_____, at ____H____

Name and signature of the person who has received the request

APPENDIX 4

TRANSMISSION FORM FOR DATA SUBJECTS' REQUESTS TO EXERCISE THEIR RIGHTS TO THE CONTROLLER: *Company X* (EXTERNAL)

Details of the person who has received the request:

- Request received on: ____/____/_____, at ____H____
- Request received by:
- Company: *Company X*
- Department:
- Capacity (service provider, supplier, developer, hosting company, etc.):
- Controller:

Details on the data subject:

- Last name:
- First name:
- Postal address:
- Telephone:
- Email address:
- Other information stated:

Details on the request:

- ***Type of request*** (tick the request submitted by the data subject – it is possible to tick more than one box – and state if the data subject has specified the request)
 - Request for access:
 - Request for rectification:
 - Request for deletion / erasure:
 - Request for portability:
 - Request for restriction of the processing:
 - Request to oppose the processing:
 - Request to organise instructions following death:
- ***Request sent to the S2H Group DPO on:*** ____/____/_____, at ____H____

Name and signature of the person who has received the request