DIOTSIACI

GDPR

Personal Data Protection Policy

GENERAL INFORMATION

Date	28/03/2018
Title	Personal Data Protection Policy (PDPP)
Issuing division	Legal, Risk and Compliance Division Data Privacy Team
Approved by	Legal, Risk and Compliance Division
Person(s) in charge of document	Santiago VALLS DPO – Legal Expert Valérie ANTOINE Group Deputy DPO – Compliance Project Manager
Dissemination	Public information

This document is disseminated among all internal departments of the Diot-Siaci Group and may be disseminated as part of business relations (clients, risk carriers, sub-contractors).

Versions	1st version: 28/03/2018 2nd version: 29/10/2018 3rd version: 08/03/2019 4th version: 24/06/2019 5th version: 03/03/2020 6th version: 30/03/2021 7th version: 25/08/2022 (updated on 06/09/2023)

Contents

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 *(Article 4.7 of GDPR)*.

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 *(Article 4.15 of GDPR)*.

DPO Data Protection Officer *(Article 37 of GDPR)*

GDPR General Data Protection Regulation. As this is a European Regulation, it is directly applicable in the legal system of European Union Member States.
In France, it is included in the Law No. 78-17 dated 6 January 1978 on IT, files and freedoms.

NIR *Numéro d'Inscription au Répertoire national*, a natural person's French social security identification number.

Personal Data Any information relating to an identified or identifiable natural person ('Data subject') *(Article 4.1 of GDPR)*.

Processor A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller *(Article 4.8 of GDPR)*.

Sensitive Data Under the GDPR, Sensitive Data concerns:

- 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.

(Article 9 of GDPR)

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 1978[1]. Personal Data protection is a key issue on both a European level, with the Directive dated 24 October 1995[2], and a national level as this Directive was transposed into French legislation by the Law dated 6 August 2004[3] (which amended the French Data Protection Act) and amended by the Law No. 2018-493 dated 20 June 2018 on Personal Data protection[4].

The General Data Protection Regulation (hereafter GDPR)[5], which entered into force on 24 May 2016 and became 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 the Diot-Siaci Group (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 year[6].

1.2. Internal background

Diot-Siaci is one of the leading providers in France in insurance consulting and brokerage services specializing in health & life and property & casualty risks, in particular for companies.

In certain situations, the Group may act as a controller or an independent joint controller and in others as a processor. Aware of the challenges raised by these different roles, the 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.

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')"[7] .

As part of its business, in particular for health and life insurance but also in the event of the administration of a "personal injury" insurance file, the Group must collect and handle Personal Data such as first and last names, age, address or

[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.

[5] 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.

[6] Article 83 GDPR.

[7] Article 5 GDPR.

French social security identification number (NIR – *Numéro d'Inscription au Répertoire national*) and also so-called "Sensitive" Data[8].

Sensitive Data

Under Article 9 of the GDPR, Sensitive Data concerns:

- racial or ethnic origin;
- political opinions, religious or philosophical beliefs or trade-union membership;
- health[9], sex life or sexual orientation;
- Genetic Data;
- Biometric Data for the purpose of uniquely identifying a natural person.

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.
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 supervised. 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, referred to as the "IT Charter". The Group undertakes to process Data in a confidential manner. To achieve this, access to the information system is subject to authorisation and is monitored[10].
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 information[11]), 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 GDPR;
- The hosting of Health-related Data;
- Defence-related classified information.

[8] Article 9 GDPR

[9] 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*".

[10] Art 32,4° GDPR.

[11] 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.

4. Detailed organisation regarding Personal Data protection

4.1. Organisation regarding Personal Data protection

The GDPR requires the Diot-Siaci Group to appoint a Data Protection Officer (DPO) for companies processing a considerable volume of Personal Data, and/or Sensitive Data.
In order to ensure the best possible management of compliance by all its companies subject 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 an Information Systems Security Manager (hereafter ISSM) in order to ensure that Data protection is dynamic and effective across the Group. A Personal Data Committee has also been created.

4.2. Roles and responsibilities

a. The DPO

The GDPR stated that the appointment of a Data Protection Officer (DPO) was mandatory if:

- the entity is a public body;
- the entity is a company whose core activity involves large-scale, regular and systematic monitoring of people, or large-scale processing of "Sensitive" Data or Data related to criminal convictions or offenses[12].

The CNIL highly recommends that, even if the body is not officially obliged to appoint a Data Protection Officer, it appoints a person who has internal representatives, responsible for ensuring compliance with the European regulation.

The Data Protection Officer is a major asset to understand and comply with the obligations of the regulation, to communicate with the Data protection authorities and to reduce litigation risks.

The DPO is chosen by the company based on 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.).

The Group DPO is the Group's Legal, Risk and Compliance Director. She reports to the Corporate Managing Director, who is a member of the Diot-Siaci Group's Executive Committee and who reports directly to the Chairman.

The DPOs of several insurance brokerage companies of the group report to her.
The Group DPO and the abovementioned DPOs are collectively referred to as "the DPO".

The Group DPO (i) coordinates the actions of the Data Privacy team and (ii) leads the Personal Data Committee.
She plays a central role considering the importance of the subject and the issues to be addressed.
The scope defined for the involvement of the DPO and her team is as follows:

- The DPO is the CNIL's registered contact for named Group companies. She is responsible for implementing compliance with the GDPR for these companies;
- As Group DPO, the DPO assists the local correspondent for French subsidiaries for which a DPO is not officially required;
- For European subsidiaries outside of France, she assists the local correspondent where required.

The DPO keeps a register of processing in which all Personal Data processing actions conducted by the Group's subsidiaries and entities in France for which she is the registered contact are listed.

(i) The DPO must be consulted prior to the implementation of any new Personal Data processing ("New Project" form in APPENDIX 3).

[12] Article 37.1 c) GDPR

The DPO ensures compliance with the applicable Data protection legislation.
Her opinions and recommendations must be sought before any new project is rolled out.

(ii) It is the DPO's role to discuss Data protection, on a regular basis and depending on the subject, with the various corporate divisions (Information Systems Division, Financial Division, Human Resources Division, Communications Division, etc.) as well as with the various Data Protection Correspondents (DPC) appointed within each business line or department in the Group's entities and the Information Systems Security Manager (ISSM) within the Information Systems Division.

(iii) The DPO issues instructions to compliance officers in the Group entities for which she is not the CNIL's registered contact in France.

The DPO's role within the Group includes in particular:

- Leading and coordinating the Personal Data protection procedure;
- Contributing to 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.

(iv) 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.

(v) The DPO and her team (Data Privacy Team), in association with the Training department of the Human Resources Division, conduct awareness-raising initiatives for Diot-Siaci Group employees and where necessary provide training through ad hoc sessions.

For the performance of all these duties, the DPO must ensure that her skills are maintained by keeping abreast of the latest Personal Data protection developments. 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 each entity which is not obliged to appoint a DPO 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 are the first to 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;
- act as members of the Personal Data Committee.

The Compliance Officers of the Group's international subsidiaries may also be more appropriate points of contact for the Group DPO.

c. The Information Systems Security Manager (ISSM)

The ISSM ensures compliance with Data protection obligations on a day-to-day basis within the Information System (IS). He/she:

- manages the Data protection approach in the Information Systems (IS);
- instigates bottom-up and top-down feedback with the DPO;
- takes part in regular discussions with Data Protection Correspondents (DPCs).

A monthly meeting is organized on a regular basis with the DPO and the Data Privacy Team, to which the Information Systems Director is invited, to enable the sharing of information and better implementation of Personal Data protection.

d. The Legal Division

The Group 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.

e. The Data Privacy team

The Data Privacy team assists the DPO with all her duties regarding Personal Data protection within the Group.
For example, the Data Privacy team is in charge of participating in the update of the central internal documentation (feedbacks from the Business lines to update the Group processing register, recording of the Impact analyses on Data protection for previous and new processing actions carried out by the Data Protection Correspondents, analysis of incidents related to Data, etc.).

f. The Information Systems Division

The Group Information Systems Division (hereafter ISD) assists the DPO in the performance of her duties and provides expertise on the securing of the Information System's applications and architecture principles together with the ISSM.
The main roles of the ISD as regards 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:

- approves structuring options and expected arbitration regarding Personal Data protection;
- sets the objectives and direction of the Group's regulatory compliance;
- is informed of the recorded incidents and gaps of compliance, if any, as well as of the remediation plans implemented to bridge any said gaps to the best of the company's capacity of action (budget, dedicated staff, projects to be launched, software overhaul schedule, etc.).

This Committee is led by the Group DPO and is comprised of:

- All members of the Data Privacy team;
- The Information Systems Director;
- The Information Systems Security Manager;
- The Communications Director;
- The Innovation and Growth Director;
- The Data Protection Correspondents of Corporate and Business lines;
- One or several occasional guests depending on the agenda.

The Data Protection Committee meets four (4) times a year and has the option of convening an emergency Committee meeting in the event of an issue that must be resolved swiftly.

The Diot-Siaci 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 provided to all employees, first via a mandatory e-learning module included in the training program of the Group's new employees, which is then updated on a regular basis through regular messages on the Group Intranet, dedicated newsletters and important reminders via Group emails according to the needs, and targeted emails to the Data Protection Correspondents within the business lines.
Awareness-raising presentations on GDPR in department or team meetings were provided as of January 2018 and are still organized where necessary.

According to the ISSP, employee training and awareness-raising initiatives concerning Information System Security (hereafter ISS) are key ISS activities and must mitigate risk exposure.
The Information Systems and Human Resources Divisions ensure that:

- documents on security are disseminated and presented to all employees,
- the IT Charter, which constitutes an annex to the in-house rules and regulations of the Economic and Social Unit (UES), is disseminated to all employees, who adhere to the Charter by signing it,
- employees enjoy and are aware of the means to access documents on security 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 Diot-Siaci 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 Diot-Siaci 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 Data.
For direct collection (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 1). 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[13];
- 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 (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.

[13] Article 85 of the French Data Protection Act, amended by the French law for a digital republic

5.2. Data processing declarations to the CNIL

The GDPR has repealed the CNIL's previous Data processing pre-declaration scheme.
It is now the Group's duty to conduct Privacy Impact Assessments on Data subjects in order to measure the risk raised by the implementation of 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).

5.3. Privacy Impact Assessment

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

- 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 Diot-Siaci 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.
The 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 risk.

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

All processing of Personal Data conducted within the Group must comply with protection rules 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 ISSM. This document also sets out the security measures applicable to the Diot-Siaci 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 Diot-Siaci 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.

Teleworking employees access the company via the secure platform CITRIX which includes all the protections described in the Personal Data Protection Policy (PDPP), or using a VPN.
The Group's ISSP provides for mobile access under the following conditions:

- only mobile access means approved by the ISD must be used.
- no simultaneous access: when mobile access to the company's IS is effective, any other communication must be blocked.
- authentication of the mobile access: any mobile access to the company's IS must be subject to strong authentication requirements.
- confidentiality and integrity of flows: any mobile access must ensure confidentiality and integrity of the flows between the mobile equipment and the IS being accessed.
- use tracking: any use must be tracked (mobile access to be specified).
- secure workstations: workstations must be equipped with an antivirus program and a firewall. Updates must not be blocked.
- raise awareness among employees: employees must be made aware of the best uses and risks resulting for example from the absence of update of an antivirus program, mixed use of personal and professional mailboxes, or storage of corporate Data on public platforms.
- control the different types of use: the implementation of a Charter within the company which sets out best practices, details restrictions and presents the procedures to be complied with.

5.5. The specific case of the NIR identification number and Data on health

For business related to administration of healthcare costs, 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 by contacting the medical departments within the business lines. In addition, the hosting company selected by the Group is certified "Hosting for Health-related Data".

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 and a right to rectification 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.
All natural persons enjoy the right to erasure 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 and oppose the processing operation.
Persons also have the right to Data portability 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, 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, 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. 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 her team members. The DPO can be contacted by email (at the following address: **dpo@s2hgroup.com**). The DPO information procedure explains how and when the Group DPO should be contacted.
A transmission form for Data subjects' requests to exercise their rights (APPENDIX 4 and APPENDIX 5) 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 Diot-Siaci 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 Information System, 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 Data 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 decision;
- The controller has provided appropriate safeguards and has informed Data subjects of the transfer, and enforceable Data subject rights and effective legal remedies are available. Appropriate safeguards may include the implementation of binding corporate rules (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 Diot-Siaci 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.

5.8. Processors

The GDPR pays special attention to the use of processors.
As part of the contracts signed with its processors tasked with processing Personal Data on its behalf (or of a Group entity), the Diot-Siaci 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 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.
The service contracts of processors come with an annex on the GDPR produced by the Legal Division to ensure that all requirements under the European regulation are impacted on the processor supplier or provider.
According to the Group ISSP, a service contract is signed between Diot-Siaci 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 processing.
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 Diot-Siaci 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 protection

In order to be able to ensure the Diot-Siaci 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 3) to allow the teams responsible for new projects to notify the DPO of the project in question and to receive her advice.

5.11. Management of incidents/flaws/Data breaches

In the event of a security incident, Diot-Siaci has implemented an Incident-Flaw-Breach 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;
- 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.

As Processor, the Diot-Siaci Group undertakes to notify the Controller, as soon as possible after becoming aware of it, of any security breach leading to accidental or illicit destruction, loss, alteration, disclosure of or unauthorised access to Personal Data. In a general manner, the Group undertakes to help its Client, whenever possible and using appropriate technical and operational measures, in managing notifications of Breaches of Personal Data.

Any detection of a Breach will be quickly assessed by the Group with the implementation of a system adapted to the identification of the root cause of the Breach, with a view to preventing or mitigating the effects caused by the Breach.
When a Breach is detected, the Group will take all necessary measures to prevent these incidents from happening again.

5.12. The fate of Data once the service is completed

As controller, the Diot-Siaci Group regularly deletes Data or makes the relevant arrangements to this end according to legal requirements.
As processor, the Diot-Siaci 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 under the conditions laid down in the contractual annex on the GDPR.

5.13. Periodical compliance audits

The Diot-Siaci Group may conduct two types of audits:

- Internally, as part of the multi-year internal audit plan. The Diot-Siaci 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 Diot-Siaci 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. Diot-Siaci 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 by registered mail with proof of delivery at least thirty (30) 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: Reminder of the 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 2: Reminder of the major principles laid down by the GDPR relating to Data protection:

All of the GDPR recitals lay down the principles that must be respected to ensure the protection of Personal Data, therefore the privacy of the Data subjects.

1. Lawfulness of processing;
2. Fairness in Data collection;
3. Use of Collected Data only for the defined purposes;
4. Processing of accurate, complete and adequate Data;
5. Limited storage period according to legal requirements;
6. Security of Data thanks to a level of security appropriate to the risk;
7. An accountability approach to demonstrate the policy implemented, including compliance with the principles of Privacy by design and Privacy by default;
8. Respect for the rights of the Data subjects.

APPENDIX 3: Informing the DPO of the updates to be listed in the register of processing (Diot-Siaci Group internal use)

"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): _____
   ☐ Anonymisation mechanism: _____

□ Pseudonymisation 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 Diot-Siaci 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:
○ To which country? _____
○ 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 4: Transmission of natural persons' requests to exercise their rights to the DPO (Diot-Siaci Group internal use)

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 Diot-Siaci Group DPO on: _____/_____/_____, at ____H_____

Name and signature of the person who has received the request

APPENDIX 5: Transmission of Data subjects' requests to exercise their rights to the Controller when the Diot-Siaci Group is the Processor (Diot-Siaci Group internal use)

TRANSMISSION FORM FOR DATA SUBJECTS' REQUESTS TO EXERCISE THEIR RIGHTS TO THE CONTROLLER: Company X (Controller outside of the Diot-Siaci Group)

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 Diot-Siaci Group DPO on: _____/_____/_____, at ____H_____

Name and signature of the person who has received the request