General Personal Data Protection Policy

Fédération Handicap International – Humanity & Inclusion – 2020

Table of contents

1. Objectives and scope

All capitalised terms used in this General Personal Data Protection Policy (hereinafter referred to as the "Policy") are defined in the "Definitions" Appendix.

1.1 Policy objectives

HI has made the commitment to **guarantee the protection of the Personal Data** it obtains in carrying out its activities, and to comply with the laws and regulations applicable to Personal Data and Special Category (or Sensitive) Personal Data Processing.

This Policy's objectives are to:

- **Define HI's commitments** with regard to the principles imposed by Applicable Legislation, and in particular 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, in effect since 25 May 2018;
- **Define the roles and responsibilities** of key contributors;
- **Ensure that appropriate measures and procedures** and **appropriate governance and supervision entities** are set up to guarantee compliance with commitments and Applicable Legislation.

HI's commitments are summarised in the R0X rule boxes. HI compliance with these rules will be audited, as detailed in the "Supervision of compliance" Section.

The following Policies and Procedures complete this Policy:

- HI's Rules of Procedure and related Memorandums;
- HI's Security Breach Management Procedure;
- HI's Data Subject Rights Management Procedure;
- HI's Data Retention Policy;
- HI's Information and Communication Technology Charter.

1.2 Scope

This Policy has been designed to apply to all HI Federation and HI France staff members (employees, trainees, volunteers) and all Data Processing carried out by the Organisation under French jurisdiction.

Staff members with "headquarters employment contracts" (governed by French law) and international staff members with "international employment contracts" (entered into with HI Federation headquarters in France) are concerned by this Policy.

In the event of conflict between this Policy and Applicable Legislation, the following rules apply:

- If the Policy is more protective, the Policy must take precedence over Applicable Legislation.
- If Applicable Legislation is more protective, Applicable Legislation must take precedence over the Policy in these specific cases.

If any doubt remains, HI or an HI staff member must seek the advice of the Personal Data Protection Officer (DPO).

1.3 Policy review

This Policy will be updated by HI's DPO if there are:

- Significant changes to HI's vocational sector or HI's Personal Data protection strategy;
- Significant changes in risk exposure (e.g. new threats, new trends, etc.);
- Significant changes in Applicable Legislation.

All modifications are subject to validation by General Management. If necessary, modifications will be communicated to HI staff members in an appropriate manner.

2. Organisation and governance of Personal Data protection

All individuals within HI play an active role in Personal Data protection. Protecting Personal Data must be a constant concern, which informs operational policies, procedures and practises.

The key contributors identified in this section accept and take on their roles and responsibilities in order to ensure that this Policy is implemented in a coherent and coordinated manner within HI.

2.1 *Key contributors*

2.1.1 General management

HI's strong commitment to Personal Data protection is one of the Organisation's strategic assets. As such, Personal Data protection is safeguarded by General Management, which must:

- Ensure appropriate governance of Personal Data protection. Appropriate governance involves defining the roles and responsibilities of all individuals within HI and involving the DPO - in an appropriate and timely manner - in all data protection-related issues;
- Inform all staff members of the DPO's designation, missions and contact information;
- Ensure that the DPO:
    - Has the appropriate resources and means required to exercise his or her missions;
    - Exercises his or her missions independently;
    - Receives appropriate training;
    - Can report directly to General Management.

2.1.2 Sector-based Divisions

Within HI, any Sector-based Division manager with authority over the implementation of Data Processing operation(s) is an **Internal Mediating Data Controller (IMDC)**. (Managers can delegate this authority to an n-1 manager, using the formal authority delegation process.)

IMDC missions are the following:

- To ensure compliance with the principles and rules prescribed by this Policy and by the complementary procedures and policies.
- To designate one or more **Operational Data Processors (ODPs)** within their Division, responsible for operational implementation of Data Processing.
- To ensure the robustness - throughout the compliance process - of compliance action plans proposed by the ODP(s) and organise semi-annual reviews of actions

with the ODP(s) in his or her team. Once compliance has been achieved, and until any further compliance becomes necessary, the frequency of reviews can be adapted.
- To immediately summon a crisis unit - any time there is proven Breach of Personal Data - to address both curative and preventive issues.

Operational Data Processors (ODPs) define Data Processing purposes and implement Data Processing operations (strategic processes, operational processes, compliance and crisis management, etc.). This is done in collaboration with colleagues (in particular, their IMDC, the Information Systems Division, etc.). ODP duties are the following:

- To involve the DPO from the outset at the design phase in all new projects involving Personal Data Processing;
- To record all new Data Processing operations in HI's Record of Processing Activities;
- To define data retention periods, data anonymisation and disposal processes and present these to their IMDC;
- To define the compliance action plan and monitor its implementation with their IMDC;
- To keep a Record of Processing Activities to track Data Processing carried out under their responsibility, as described in the GDPR;
- To implement technical and organisational measures to safeguard Personal Data;
- To respond to Data Subjects when they exercise their rights, in particular to Data Subject right of access requests in compliance with GDPR requirements;
- To carry out Data Protection Impact Assessments (DPIA) if necessary, with the assistance of the DPO and any other pertinent technical expert;
- To provide written documentation and justification if DPO advice is overruled;
- To respond to all information requests made by the DPO with regard to any issue impacting Data Subject privacy;
- To provide all required documentation relating to Data Processing carried out within their perimeter of responsibility;
- To integrate Personal Data protection when drafting and negotiating contracts with external parties (contracts, NDAs, letters of intent, commercial agreements, Data Transfer agreements, etc.).

2.1.3 Data Protection Officer (DPO)

HI has appointed a **Data Protection Officer (DPO)** to ensure the Organisation's compliance with Applicable Legislation and the fulfilment of commitments made in this Policy.

The DPO's missions within HI are the following:

- To inform and raise staff member awareness of Personal Data protection rules;
- To ensure compliance with Applicable Legislation and fulfilment of commitments made in this Policy;
- To advise Sector-based Divisions with regard to the practical application of data protection principles to Data Processing projects;

- To inform, empower, and if necessary, alert General Management in relation to the risks that specific staff initiatives or non-compliance with DPO recommendations might generate for HI;
- To decide whether a Data Protection Impact Assessment (DPIA) must be performed and advise the Sector-based Division in this process;
- In the event of a Personal Data Breach, to assist in evaluating the risk generated by the Breach and serve as a contact point if the competent Supervisory Authority and/or concerned Data subjects are notified;
- To analyse, investigate, audit and control HI's level of compliance and, if necessary, support Sector-based Divisions in defining and implementing a remediation plan;
- To establish and keep up to date any documentation required by the data protection principle of accountability ;
- To guarantee appropriate administration of Data Subject rights, in compliance with the relevant Procedure;
- To present an annual report to General Management;
- To interface and cooperate with the Supervisory Authority.

The DPO may designate one or more deputy DPOs among HI staff members. The DPO must announce this designation in an appropriate manner.

2.1.4 Legal Division

The Legal Officer provides the following support and expertise:

- Clarifications and implementation instructions with respect to Applicable Legislation requirements;
- Advice regarding potential legal impacts;
- DPIA assistance (e.g. advice regarding categories of Personal Data collected, data retention periods and the Consent management process);
- Drafting of appropriate legal documents.

2.1.5 Information Systems Division

The DPO is managed by the Information Systems Division (ISD) Director.

For each project, the ISD Director provides his or her support and expertise in the following areas:

- Assessment of context and project criticality;
- Risk analysis, in particular for the DPIA pre-assessment;
- Advice regarding security measures required to reduce, avoid or transfer risks;
- Evaluation of the level of security provided by intervening Third Parties and negotiation with Third Parties for integration of HI security requirements into contract(s);
- Coordination of security incident vigilance, detection and management, under DPO guidance, if a Data Breach occurs.

2.2 *Annual DPO report*

The DPO produces and publishes an annual report summarising HI's privacy protection activities. For this reporting process, the DPO defines, collects and publishes indicators quantifying the level of compliance with relevant internal policies and procedures, and Applicable Legislation.

3. Personal Data Processing principles

In accordance with Applicable Legislation, HI commits to complying with the principles defined below when collecting and processing Personal Data.

3.1 *Principle of 'lawfulness, fairness and transparency'*

Personal Data must be collected and processed in a **lawful, fair and transparent** manner.

Therefore, HI ensures that Data Processing always rests upon a **legal basis recognised by Applicable Legislation**. Recognised lawful grounds for Data Processing include:

- Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes (subject to compliance with additional requirements detailed in this Policy's "Consent" Section);
- Processing is necessary for the performance of a contract to which the Data Subject is a party, or in order to take appropriate measures requested by the Data Subject prior to entering into a contract;
- Processing is necessary for compliance with legal obligations to which HI is subject;
- Processing is necessary in order to achieve legitimate interests pursued by HI;
- Processing is necessary in order to protect the vital interests of the Data Subject;
- Processing is necessary for the performance of a mission carried out in the public interest.

If Data Processing is based upon legitimate interest, HI must perform an analysis to determine whether this legitimate interest overrides the Data subjects' interests or fundamental rights and freedoms. This analysis and its results must be documented and recorded for probationary purposes (accountability).

Under exceptional circumstances, HI may process "Special Category (or Sensitive) Personal Data". In this case, HI must comply with the requirements defined in this Policy's "Special Category (or Sensitive) Personal Data Processing" Section.

R01 All Data Processing rests upon a legal basis that is clearly identified and documented in the Record of Processing Activities.

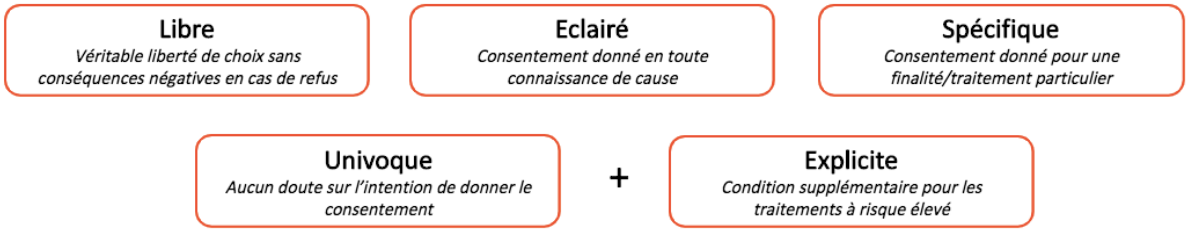
In addition, HI ensures that Personal Data Processing activities are carried out in an **apparent and transparent** manner. To this end, HI provides accessible and intelligible information to Data Subjects regarding how their Personal Data is used, in accordance with the Data Subject Rights Management Procedure's terms and requirements (cf. this Policy's "Data Subject Relations" Section).

3.2 *Consent*

When Data Processing is based upon Data Subject Consent, HI ensures that Consent is obtained legally (please consult the "Consent Validity Requirements" Section) and is properly managed throughout the entire Data Processing process (please consult the "Consent Management" Section).

3.2.1 Consent Validity Requirements (data collection characteristics and modalities)

HI ensures that Consent obtained from Data Subjects meets the following criteria:



In addition, when necessary, HI must ensure compliance with local laws legislating the validity of Consent.

Consent must be obtained prior to Data collection or, if not, *no later than* at the time of Data collection. Consent requests must be distinguished from all other requests/issues, and formulated in an intelligible and easily accessible manner, in clear and plain language.

R02 When the legal basis for Data Processing is Consent, Consent obtained must meet content (characteristics) and format (collection) validity requirements.

3.2.2 Consent management (duration, evidence)

HI ensures compliance with the **period of Consent validity**. Indeed, if Data Processing modalities change or evolve, original Consent is no longer valid. When Consent is no longer valid, it must be obtained again.

As far as possible, HI **tracks** the **declarations of Consent** that it receives. To this end, HI keeps a record of who gave Consent, how Consent was obtained and when Consent was obtained, as well as a record of the information provided to Data Subjects at the time of Consent.

R03 If Data Processing modalities change significantly, Consent must be renewed.

R04 A system is implemented to track Declarations of Consent.

3.2.3 Withdrawal of Consent

Data Subjects must be able to **withdraw their Consent at any time**. HI must provide Data Subjects with the means to withdraw Consent as easily as it was given. As far as possible, this must be done using a method equivalent to that used to obtain Consent.

Once Consent is withdrawn, HI must ensure that Consent **withdrawal is recorded in its systems** and databases without undue delay, so that the Personal Data is no longer processed for the purpose in question (e.g. a VIP member who has withdrawn image use Consent should no longer see their image exploited). In addition, any change in Consent status must be **communicated to all third-party stakeholders**, and in particular to Processors, so that they no longer process the Personal Data in question for the purpose in question.

Once Consent is revoked, HI can no longer use Consent as the legal basis for Data Processing. However, withdrawal of Consent

- Does not affect the lawfulness of Data Processing prior to withdrawal of Consent,
- Does not necessarily require Personal Data deletion if Data might still be useful for other Data Processing purposes and/or be of administrative interest.

R05 Data Subjects are able to withdraw their Consent at any time as easily as Consent was given.

R06 Withdrawal of Consent is integrated effectively into Data Processing tools.

3.3 *Principle of 'purpose limitation'*

HI must clearly define data collection purpose(s) prior to Personal Data collection. Purpose(s) must be **specified, explicit and legitimate**. HI must also ensure that pursued purpose(s) are compatible with its activities.

Personal Data must not be further processed for purpose(s) incompatible with the initial purpose for which Data was collected. Therefore, HI must perform a **compatibility test** to check whether the purpose for further Data Processing is compatible with the initial purpose. Testing must take into account the following:

- Potential connection(s) between both purposes;
- The context in which Personal Data was collected. In particular, the relationship between Data Subjects and HI;
- The nature of Personal Data. In particular, whether processed Data is Special Category (or Sensitive) Personal data;
- Potential consequences for Data Subjects of contemplated further Data Processing;
- Existence of appropriate guarantees.

When the purpose of further Data Processing is incompatible with the initial purpose, HI must obtain Data Subject Consent, in compliance with the requirements of Applicable Legislation (Article 6(4) of the GDPR).

R07 Personal Data is collected for only specific, explicit and legitimate purpose(s), and must not be further processed in a manner that is incompatible with (initial) purpose(s).

3.4 *Principles of 'data minimisation' and 'accuracy'*

Personal Data collected must be **adequate, relevant and limited** to what is necessary in relation to the purpose(s) pursued by Data Processing. In other words, HI ensures that only Data **strictly necessary** to achieve the purpose(s) is collected.

Furthermore, HI ensures that Personal Data is **accurate and, where necessary, kept up to date**. To this end, HI takes **every reasonable step** to erase or rectify inaccurate Personal

Data without delay, and without losing sight of Data Processing purpose or the associated need for accurate Data.

R08 Personal Data is adequate, relevant and limited to what is necessary in light of Data Processing purpose. Personal Data is accurate, complete and kept up to date if necessary.

3.5 *Principle of 'storage limitation'*

HI ensures that processed Personal Data is **retained no longer than is needed** for the purposes for which it is collected.

Personal Data may be retained:

1) In a format that enables Data Subject identification for a **period not exceeding the length of time required for Data Processing purposes**. Therefore, once the purpose is fulfilled, Data must be **deleted**.

2) Longer than the length of time required for Data Processing purposes, if data remains of **administrative interest**. The data retention period may in this case be extended beyond the period deemed fitting for the initial collection purpose. Data retention period extensions must be duly **justified and documented**.

   Data may also be retained to comply with **statutory limitation periods**, **specific data retention times** (retention of accounting documents and supporting documents, archiving of electronic contracts, etc.), mainly for **probationary purposes**, or in order to **respond to communication requests** that might be made by legally authorised Third Parties (e.g. tax authorities, social service agencies, etc.).

3) For **longer periods**, insofar as Personal Data is processed exclusively by HI for **archiving in the public interest or scientific or historical research purposes**, provided that appropriate technical and organisational measures are implemented (such as **anonymisation** or **pseudonymisation**) to guarantee Data Subject rights and freedoms.

To ensure compliance with the principle of restricted data retention, HI defines applicable data retention periods for Data Processing operations. For each category of Data collected, the following must be considered when determining data retention periods:

- Legal obligations;
- The recommendations of the French Supervisory Authority, the CNIL (*Commission nationale de l'informatique et des libertés* - National Commission for Information Technology and Freedoms);
- Best practises in the field in question;

- HI's operational needs.

Data retention periods are **reviewed and updated whenever necessary** to reflect evolutions in Applicable Legislation and/or HI practises.

Once the data retention period has elapsed, Data is **deleted without undue delay**. Data can be deleted via destruction and/or anonymisation. If Data is deleted via destruction, HI ensures that is truly removed from all systems (including third-party systems).

Restricted Personal Data retention implementation requirements and procedures are defined in HI's "Data Retention Policy".

R09 Data retention periods are defined and implemented. HI implements a Data Retention Policy.

3.6 Personal Data security

HI takes **technical and organisational measures** to ensure Personal Data **security, confidentiality and integrity** throughout the entire Data Processing process. These measures are defined based on the following:

- Likelihood and severity of potential damage in the event of data loss, alteration or unauthorised access;
- Specific characteristics of Data Processing operations;
- If relevant, the results of the Data Protection Impact Assessment;
- State-of-the-art guidelines and practises;
- Implementation costs.

HI commits to reviewing security measures regularly in order to **test, evaluate and determine their effectiveness and make necessary improvements**.

HI also ensures that all Data Breaches are managed correctly in accordance with this Policy's "Data Breach Management" Section.

R10 Appropriate technical and organisational measures are implemented to ensure Personal Data security, confidentiality and integrity.

3.7 Personal Data transfers to countries outside the European Union

All Transfers of Personal Data require additional attention and guarantees. HI ensures that all Personal Data Transfers are **appropriately secured** and **executed lawfully** in compliance with the requirements of Applicable Legislation.

To this end, HI ensures that it:

- **Identifies all Personal Data Transfers**, including, wherever possible, onward Transfers performed by (1st rank) Processors;
- **Oversees in each service provider contract** all Data Transfer operations and, when necessary, Data hosting locations (on principle, located within the European Union). It is required that all service providers guarantee the implementation of measures ensuring Personal Data protection levels equivalent to that provided by the GDPR;
- **Safeguards all Data Transfers** by implementing appropriate technical and organisational measures;
- Legally supervises the Transfer using an **appropriate mechanism** when Data is transferred to a country not recognised as adequate (i.e. European Commission has not made an adequacy decision).

As far as possible, Personal Data must not be automatically transferred to a country outside the European Union without the authorisation of HI's DPO.

R11 All Personal Data Transfers are appropriately secured and executed lawfully in compliance with the requirements of Applicable Legislation.

3.8 Special Category (or Sensitive) Personal Data Processing

In addition to the general requirement for a legal basis (please consult the "Principle of 'lawfulness, fairness and transparency'" Section), Special Category (or Sensitive) Personal Data can only be collected IF one of the following **special conditions** apply:

- Data Subject has given explicit Consent;
- Processing is necessary to fulfil obligations and/or exercise HI or Data Subject rights related to labour law, social security or social protection;
- Processing is necessary to safeguard the vital interests of the Data Subject;
- Processing is carried out by a foundation, organisation or any other non-profit body to pursue a political, philosophical, religious or trade union purpose, within their legitimate activities and with appropriate guarantees;
- Processing relates to Personal Data manifestly made public by the Data Subject;
- Processing is necessary for the establishment, exercise or defence of a legal claim;
- Processing is necessary for important reasons of public interest and based on European Union or Member State legislation. Legislation must be proportionate for the pursued objective, respect the essence of the right to data protection and provide

for appropriate and specific measures safeguarding Data Subject fundamental rights and interests;
- Data Processing is necessary for the purposes of preventive medicine, occupational medicine, assessment of occupational work capacity, medical diagnoses, health care, social care or health care system/service management;
- Data Processing is necessary for reasons of public interest in the field of public health;
- Data Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- A specific condition provided for by local legislation applies.

HI must implement **specific security measures** for Special Category (or Sensitive) Data based on the potential risk for the Data Subject.

On principle, data relating to criminal convictions, offences or related security measures must not be collected, except in extremely exceptional cases, and with DPO validation (e.g. obtaining criminal records to verify job applicant information relating to the specific nature of the employment position). This type of Special Category (or Sensitive) Personal Data cannot - in any event - be processed (i.e. copies of criminal records may be collected, but may not be retained).

R12 Special Category (or Sensitive) Personal Data Processing is on principle prohibited. Exceptions to this rule can only be made in compliance with the requirements of Applicable Legislation, and validated by the DPO. .

4. Risk management and documentation

All evidence of regulatory compliance must be safeguarded in order to demonstrate HI's compliance to the Supervisory Authority.

4.1 *Privacy by Design/by Default*

For all new projects involving Personal Data Processing, HI implements appropriate Personal Data protection measures, from the outset at the Data Processing process design stage and throughout the project and Personal Data life cycle (from collection to destruction).

To this end, HI staff members responsible for a project must take the following steps:

Etape 1. Verify that the principles defined in this Policy's Section 3 are respected.
Etape 2. List existing and foreseen technical and organisational measures that will safeguard Personal Data security, confidentiality and integrity.
Etape 3. Carry out a preliminary evaluation prior to the Data Protection Impact Assessment.

Etape 4. If necessary, carry out a Data Protection Impact Assessment.
Etape 5. Implement security measures adapted to the level of risk.

When the project involves completely or partially entrusting Data Processing to a Processor, HI ensures that the requirements defined in the "Intervening Third party Management" Section are respected.

R13 All projects integrate Personal Data protection from the outset at the design phase and by default.

4.2 *Data Protection Impact Assessment*

When Data Processing is likely to generate a **high level of risk** for Data Subject rights and freedoms, HI performs a **Data Protection Impact Assessment** (DPIA), **prior to implementing Data Processing**.

HI also ensures that a **preliminary evaluation** is performed for all new Data Processing operations to determine the Data Processing risk level and establish whether a DPIA must be performed. Preliminary evaluations take into account:

- The cases in which a DPIA is mandatory, as defined in the GDPR and by the Supervisory Authority;
- The criteria defined by the European Data Protection Board;
- The exemptions and derogations relating to specific situations provided for in the GDPR and by the Supervisory Authority.

The DPIA must be **documented** and must at *least*:

- Describe Data Processing nature, scope, context and purposes;
- Assess necessity, proportionality and compliance measures;
- Identify and evaluate the risks for Data Subjects;
- Identify all additional measures required to mitigate these risks.

For further information: Please consult the CNIL DPIA Fact Sheet (in French) and HI's internal Impact Assessment management methodology.

R14 For each new project, the need for a Data Protection Impact Assessment is evaluated. If required, a DPIA is performed prior to Data Processing.

A DPIA is an **ongoing process** and must be **revisited regularly** to ensure that **risk levels remain acceptable** throughout the Data Processing life cycle. Indeed, environments, and in particular technical environments, will inevitably change. Therefore implemented measures must be adapted.

Likewise, Data Processing may sometimes not require a DPIA to begin with. However, if Data Processing operations evolve, a DPIA may be performed at a later stage.

R15 The need to update an existing DPIA or perform a DPIA is re-evaluated whenever a major change affects a Data Processing operation.

With General Management approval, the DPO **consults the Supervisory Authority** if the DPIA shows that Data Processing will result in a high risk to Data Subject rights and freedoms (i.e. if **residual risk remains high** even after definition and implementation of a risk remediation plan).

R16 The CNIL is consulted when the DPIA shows that a high residual risk remains.

4.3 Record of Processing Activities

As a Data Controller, HI must keep a **Record of Processing Activities** that is compliant with the requirements of Applicable Legislation.

All HI Operational Data Processors (ODPs) keep their Records of Processing Activities up to date under the supervision of their Sector-based Division Data Control Mediator.

To this end, HI identifies the key contributors responsible for keeping and updating the Record of Processing Activities, as well as their roles and responsibilities.

R17 A Record of Processing Activities is kept up to date.

5. Staff training and awareness-raising

HI ensures that all staff members are **aware of the importance of Personal Data protection** and understand both the intention and scope of Applicable Legislation and the risks of non-compliance.

Where possible, HI also provides **specific training** to the staff members called upon to process Personal Data on a daily basis.

Staff members are regularly provided with information and/or training relating to legislative and jurisprudential evolutions in the area of Personal Data protection, as well as on updates relating to applicable internal rules.

All new staff members undergo awareness-raising/training adapted to their missions and level of knowledge.

R18 All staff members are made aware of Personal Data protection principles and significance. More in-depth training is provided to all staff members processing Personal Data on a daily basis.

6. Data Subject relations

HI commits to guaranteeing the **effective exercise** of the rights granted to Data subjects by Applicable Legislation. Applicable Legislation grants Data Subjects the following rights:

- **Right to be informed**: the right to clear, precise and complete information regarding HI's use of Personal Data.
- **Right of access**: the right to obtain a copy of the Personal Data held by the Data Controller concerning the requesting Data Subject.
- **Right to rectification**: the right to obtain the rectification of Personal Data if it is inaccurate or obsolete and/or to have Personal Data completed if it is incomplete.
- **Right to erasure/'right to be forgotten'**: the right, under certain conditions, to have Personal Data erased or disposed of, unless HI has a legitimate interest in retaining it.
- **Right to object**: the right to object to Personal Data Processing by HI on grounds relating to the requesting Data Subject's particular situation (under certain conditions).
- **Right to withdraw Consent**: the right to withdraw Consent at any time when Data Processing is based upon Consent.

- **Right to restriction of processing**: the right, under certain conditions, to request that Personal Data Processing be temporarily suspended.
- **Right to data portability** : the right to request that Personal Data be provided to the Data Subject in a reusable format enabling it to be used in another database.
- **Right not to be subject to automated decision-making**: the right not to be subject to decisions based solely on automated Data Processing (including profiling) and having a legal impact on the Data Subject or other similar significant impact.
- **Right to give post-mortem instructions (or right to post-mortem privacy)**: the right for the requesting Data Subject to give instructions concerning the use and disclosure of their Personal Data after their death.

To guarantee the effective exercise of Data Subject rights, HI defines and implements a Data Subject **Rights Management Procedure**, in compliance with Applicable Legislation requirements. This Procedure defines:

- The standards that must be respected to ensure transparent information for Data Subjects;
- The legal requirements that must be respected;
- The channels authorised for submitting requests for each right, based on Data Subject category;
- The operational processes enabling requests to be processed in accordance with the requirements above;
- The parties involved in these processes, their roles and responsibilities.

All requests submitted by Data Subjects for the exercise of their rights are **recorded in a Data Subject Request Log** for the purpose of demonstrating compliance. The above-mentioned Data Subject Rights Management Procedure defines what this Data Subject Request Log must record and how it should be kept.

R19 A Data Subject Rights Management Procedure is applied, and eligible requests are recorded in a dedicated Data Subject Request Log.

7. Personal Data Breach management

In compliance with its security obligation, HI defines, documents and implements a **procedure to detect, qualify and respond to** Personal Data Breaches. This procedure is documented and must include:

- The use of a Data subject rights and freedoms risk assessment matrix, based on the criteria defined by the Supervisory Authority and the European Data Protection Board;
- The distribution of roles and responsibilities among all parties affected by the response plan, including Processors subcontracted by HI;

- The conditions, terms and deadlines for Data Breach notification to the competent Supervisory Authority and/or to Data subjects.

Adequate technical and organisational means are used to detect, investigate and report Personal Data Breaches. In addition, to better detect and manage Data Breaches, HI ensures staff member awareness of and training in relation to the required procedure in the event of a proven or suspected Breach.

R20 Security Breach Management Procedure is defined and implemented.

In addition, for accountability purposes, HI keeps a Security/Personal Data Breach log recording all Breaches, whether notification is required.

R21 A Security/Personal Data Breach log is kept up to date.

8. Intervening Third Party management

In compliance with Applicable Legislation, HI commits to choosing service providers offering **sufficient guarantees** for the implementation of appropriate technical and organisational measures.

To this end, **prior to selecting a service provider, HI verifies guarantees** presented by all potential third-party service providers. Verification is performed in particular via questionnaires and/or documentation analysis. The verification process must enable **the assessment of the context and circumstances in which the service provider conducts Data Processing operations**, i.e. entrusted Data Processing operation modalities, Personal Data security and confidentiality, third-party service provider maturity with regard to Personal Data protection.

R22 The guarantees offered by each third-party service provider are verified prior to implementing Data Processing activities. A Processor Conformity Assessment Matrix is used within HI.

HI ensures that intervening Third Parties are **properly qualified** (distinct Data Controller, co-controller or Processor) and that a **written contract clearly defines each party's roles and responsibilities**. This contract includes - at a minimum - the clauses required by Applicable Legislation (in particular the GDPR).

If the Third Party acts as a Subcontractor, the signed contract describes the Data Processing operation(s) entrusted to the Processor by specifying:

- Data Processing subject and duration;
- Data Processing nature and purpose;
- Personal Data category or categories;
- Data Subject category or categories;
- Instructions relating to Data Processing operations.

R23 A written contract is signed with each Third Party involved in Data Processing. The contractual agreement includes adequate relevant clauses, compliant with Applicable Legislation.

Processors are **audited regularly** to verify their continued compliance with contractual and regulatory obligations. Audit frequency and modalities are defined based upon the nature and sensitivity of entrusted Data Processing operations, required costs and available resources.

R24 Processors are audited regularly in order to verify their continued compliance with contractual and regulatory obligations.

9. Supervisory Authority relations

HI **cooperates fully with Supervisory Authorities** when required and provides exhaustive evidence of compliance with Applicable Legislation.

HI's Data Protection Officer (DPO) acts **as a contact point** for the Supervisory Authority. As such, the DPO pilots:

- Consultations with the relevant Supervisory Authority if a high residual risk for privacy is generated by Personal Data Processing;
- Data Breach reporting to the Supervisory Authority when required;
- Processing of all requests (e.g. Record of Processing Activities access requests, information requests, etc.).

HI defines a **Supervisory Authority audit procedure**, which defines the roles and responsibilities of key contributors in the event of an audit.

R25 HI cooperates with the competent Supervisory Authority and defines a procedure in the event of an audit.

10. Supervision of compliance

HI will comply with this General Personal Data Protection Policy, and with other Personal Data protection-related implementation procedures and policies.

To this end, HI **compliance with prescribed rules** and implemented Data Processing **correspondence with the Record of Processing Activities** are **verified annually**. This verification process is performed by HI's DPO and ISD Director.

If Breaches are identified, a **remediation plan** is drawn up by the DPO and all concerned stakeholders in order to remedy detected breaches. All remedial action takes into account incurred risks, implementation costs, existing and foreseeable operational constraints and available human resources. Corrective measures defined by the remediation plan are implemented by appropriate stakeholders **without undue delay**, under DPO supervision.

R26 A mechanism for supervision of compliance is set up.

R27 A remediation plan is defined and implemented to remedy all detected non-conformities.

11. HI's commitments as a Processor

11.1 *When HI is the Data Processor - Management of the Record of Processing Activities*

In compliance with Applicable Legislation, HI commits to keeping an up-to-date **Record of Processing Activities implemented for third-party Data Controllers**. This document must include the following information:

- Name and contact details of Processor, Data Controller (on behalf of whom Processor processes Personal Data) and DPO;
- Category(ies) of Data Processing carried out on behalf of each Data Controller;

- When necessary, Personal Data Transfer operations to third-party countries or with an international organisation, as well as documents attesting to appropriate guarantees;
- General description of technical and organisational security measures implemented.

This Record of Processing Activities must be updated as and when required so that it always remains **accurate and exhaustive**.

R28 A Record of Processing activities implemented by HI in its capacity as a Processor is kept up to date.

11.2 *When HI is the Data Processor - Additional obligations*

In carrying out its activities, HI acts as a Processor for third-party Data Controllers. In this case, **specific obligations** must be complied with, whereby HI:

- **Maintains a Record of Processing activities** implemented in the name and on behalf of Data Controllers (cf. previous section);
- **Acts in accordance with the lawful instructions** of the Data Controller;
- **Establishes a contract** with the Data Controller, in compliance with the provisions of Applicable Legislation;
- **Ensures the application of Personal Data protection principles from the outset at the design phase and by default**;
- Requires staff members responsible for Data Processing activities to enter into a **confidentiality agreement**;
- Respects **contractual obligations** relating to recruitment of any **subsequent Processors performing further Data Processing;**
- Integrates the **measures required to report Data Breaches to Data controller(s)** into the Data Breach Management Procedure;
- Takes the **adequate technical and organisational measures to guarantee a level of security adapted to the risks**;
- On Data Controller's instructions, **removes or restores all Personal Data** managed by the Data Controller, unless there is a legal obligation to retain the data (non-personal data attesting to the proper performance of services may be retained for the duration of the commercial action's statutory limitation period);
- **Assists, alerts and advises** the Data Controller by:
    - Informing the Data Controller when an instruction is likely to breach Applicable Legislation ;
    - Helping the Data Controller respond to Data Subject requests (financial compensation may be requested from the Data Controller);
    - Providing all available information to enable the Data Controller to carry out a Data Protection Impact Assessment and comply with Personal Data Breach management obligations (financial compensation may be requested from the Data Controller) ;

- Provide **evidence of compliance** to the Data Controller and **facilitate the performance of an audit** (abiding by the terms and conditions provided for in the Contract).

R29 HI implements the additional obligations that result from its role as a Processor.

Appendix 1 Definitions

Applicable Legislation: All regulations relating to the Personal Data protection and applicable to the Personal Data Processing carried out by HI. Namely: European 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, known as "GDPR", Legislation n°78-17 of 6 January 1978 relative to information technology, data files and civil liberties as amended by Law n°2018-493 of June 20 2018 and promulgated on June 21 2018 taking the GDPR into account and transposing the "Law Enforcement" Directive, and any other related regulation, applicable to HI.

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her; and present clients, prospective clients, and staff members.

Data Controller: Natural or legal person who, alone or jointly with others, determines what Personal Data is processed, and the purposes and means of Personal Data Processing.

Data Processing: Any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, access, recording, copying, transfer, conservation, storage, alignment or combination, alteration, structuring, disclosure by transmission, dissemination or otherwise making available, communication, erasure or destruction, whether by automated or other means (non-exhaustive list).

Data Protection Impact Assessment (DPIA): Analysis that must be carried out by HI when Data Processing is liable to generate a high risk to the rights and freedoms of natural persons.

Data Protection Officer (DPO) - cf. 2.1.3: The person designated by HI as responsible for Personal Data protection within HI and HI compliance with Applicable Legislation.

Data Recipient: Natural or legal person, public authority, agency or another body to which Personal Data are disclosed, whether a Third Party or not.

Data Subject: An individual to whom the Personal Data relates and who can be identified or is potentially identifiable, directly or indirectly, via his or her Personal Data. Data Subjects include past and present clients, prospective clients, and staff members.

Data Transfer: Any communication, copy or movement of Data via a network; any communication, copy or movement of Data from one medium to another, whatever the medium; any communication, copy or movement of Personal Data to a non-EU Member State or to an international organisation - where the Data are Processed or intended to be Processed following the Transfer.

GDPR: Abbreviation of European 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.

Internal Mediating Data Controller (IMDC) - cf. 2.1.2: at HI, each Professional Division manager is an Internal Mediating Data Controller (IMDC), insofar as the manager in question has authority over the implementation of any Personal Data Processing.

Operational Data Processor (ODP) - cf. 2.1.2: Natural person who jointly with others (in particular their IMDC, DPO, the Information Systems Division…) defines the purposes and implements Processing means (strategic chain, operational chain, implementation of compliance and crisis management…).

Personal Data: Any information relating to an identified or identifiable natural person ('Data Subject'), where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, an identity card number, a salary, health records, bank account information, behavioural or consumer habits, location Data, an online identifier, etc. The term "Personal Data" includes Special Category (or Sensitive) Personal Data.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Processor: Any natural or legal person, public authority, agency or another body which processes Personal Data on behalf of the Data Controller, in compliance with their instructions (e.g. providers, vendors or suppliers).

Special Category (or Sensitive) Personal Data: Personal Data revealing or based upon:

- Racial or ethnic origin, political, religious or philosophical opinions;
- Membership of a trade union organisation;
- Physical or mental health;
- Sexual orientation or sex life;

- Genetic and biometric data;
- Data relating to criminal convictions, offences or related security measures.

Supervisory Authority: An independent public authority provided for by a Member State in accordance with Article 51 of the GDPR, responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to Data Processing and to facilitate the free flow of Personal Data within the European Union. In France, this Supervisory Authority is the CNIL.

Third Party: Any natural or legal person, public authority, agency or other body than the Data Subject, the Data Controller, the Processor and the persons who, under the Data Controller's or Subcontractor's direct authority are permitted or authorised to process the Data.