LEYTON
Empower your future

Binding Corporate Rules (BCR)

Processor

SOMMAIRE

ARTICLE 2 : DEFINITIONS

When they commence with a capital letter, the terms appearing below shall have the following meaning:

"**Adequate Third Country**": a country which is not a member of the European Economic Area and which has been recognised as guaranteeing an appropriate level of protection for Personal Data by the European Commission in accordance with Article 45 of the GDPR;

"**BCR Entity or Entities**": an Entity or Entities which undertake to observe these BCRs by signing them, either in the capacity of a Data Exporter or a Data Importer;

"**Client(s)**": the physical person or legal entity that has signed a Service Agreement with an entity of the Leyton Group;

"Data Controller(s)": the Client(s) which determine the Purposes and the means of the Processing;

"**Data Exporter**": an Entity or Entities of the Leyton Group located in the European Economic Area which transfer Personal Data to a Third country in the capacity of a Processor;

"**Data Importer**": an Entity of the Leyton Group established in a Third country and which receives the Data in order to process them in the capacity of a Processor or Subprocessor

"Data Protection Officer" or **DPO** : the person delegated for the protection of data, established by Articles 37 et seq. of the GDPR; for the entities which will select or have already designated a DPO, this person shall ensure in particular the provision of advice and information as well as monitoring that the rules resulting from the GDPR are observed within the Entity;

"Data Protection Regulations": the unit comprised of the GDPR and the Law on Data Files and Liberties or any other specific national legislation concerning the protection of Personal Data that is applicable to each Entity over which the Data Importer agrees to have the GDPR prevail in the event of a contradiction;

"**Data Subject**": a physical person to which the Data subject to the Processing relate;

"**Entities**": Designates:

- Thésée, a French simplified joint stock company (*société par actions simplifiée*), with its registered office located at 16 boulevard Garibaldi, 92230 ISSY LES MOULINEAUX, registered with the Registry of Trade and

Companies of Nanterre, under the number 504 868 399 (hereafter referred to as "Thésée");
- Any company controlled by or controlling Thésée, in the sense of Article L.233-3 of the Commercial Code.

"The European Economic Area" or "EEA": the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway; excluding Switzerland).

"GDPR": REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC;

"**Leyton Group**": designates all of the Entities;

"**Member State(s)**": sovereign Member State(s) of the European Economic Area;

"**National Commission on Information Technology and Liberties**" (*Commission nationale de l'informatique et des libertés*) or the "**CNIL**": the French Supervisory Authority which is the BCR Lead Supervisory Authority;

"Personal Data" or "Data": any information concerning a physical person which may identify such persons directly or indirectly such as - for example - a last name, first name, initials, photos, badge numbers, or an IP address;

"Personal Data breach" : 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;

"Personnel": any physical person who is an employee, intern or other and who works on behalf of one of the Entities of the Leyton Group, with the exclusion of the Subprocessor;

"**Processing of Personal Data**": any operation or any group of operations carried out at the initiative of the Data Controller and concerning the Data, regardless of the procedure used, and in particular the collection, recording, organisation, retention, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of provision, the alignment or combination, as well as the locking, deletion or destruction;

"Purpose(s)": the objective sought by the Processing. In other words, the reasons why the data were collected by the Data Controller;

"Service(s)": any operation carried out on behalf of the Clients of the Leyton Group consisting of:

- The provision of tax and social engineering advice, particularly by means of a search for financing, optimisation of social charges, taxes and procurements (telephony, automobile fleet, temporary staffing, insurance, energy, etc.);
- The valuation of energy certificates and the provision of advice concerning energy savings;
- The provision of outsourced services in the area of human resources and invoicing/ recovery of receivables from Clients.

"**Services Agreement**": The Agreement between the Client and an Entity of the Leyton Group and which addresses the performance of the Services, for which these BCRs form an integral part;

"Processor": the physical person or legal entity, public authority, service or other body which processes the Personal Data upon the instruction of and on behalf of the Data Controller;

"Subprocessor": the physical person or legal entity, public authority, service or other body engaged by the Processor in order to process the Personal Data in accordance with the instructions of and on behalf of the Data Controller. The Subprocessor may be internal or external to Leyton Group ;

"**Supervisory Authority or Authorities**": the independent public authority or authorities established within each EEA Member State in order to protect the fundamental rights and freedoms of individuals with regard to the Processing of Personal Data within the EEA;

"**Third country** ": a country which is not a member of the EEA and which has not been recognised as guaranteeing an appropriate level of protection for Personal Data by the European Commission in accordance with Article 45 of the GDPR;

"Transfer of Personal Data" or "Transfer": any access, communication, copy or displacement of the Personal Data with the purpose of being processed in a Third country.

ARTICLE 3 : PRESENTATION OF THE LEYTON GROUP

The structure of the Leyton Group, as well as the identity and the contact information for each Entity comprising it appear in Annex 1 to these BCRs.

This Annex may be updated for each development in the Leyton Group and will be communicated to the Supervisory Authority, without the need to submit this new version of Annex 1 for the signature of each Entity that is already a party to the BCRs.

ARTICLE 4 : SCOPE OF APPLICATION

Article 4.1: MATERIAL SCOPE OF APPLICATION

These BCRs are binding on all of the Entities of the Leyton Group, whether Data Importer or Data Exporter, which has undertaken to comply with them and which has signed the adherence form appearing in Annex 0, and a list of which appears in Annex 1. In case of modification, the rules that will be applied are detailed in ARTICLE 11 : .

Article 4.2: TERRITORIAL SCOPE OF APPLICATION

These BCRs apply to the BCR Entities established in an EEA country exporting Personal Data directly or indirectly, and to the BCR Entities not established in an EEA country importing the Personal Data. The BCRs apply to first Transfers of Personal Data and to the onward Transfers

The BCRs do not apply to Transfers of data between Entities located in an Adequate Third Country or in a EEA Member State, or to Entities located in an Adequate Third Country or a EEA Member State.

ARTICLE 5 : DESCRIPTION OF THE PROCESSING ACTIVITIES

Article 5.1: DESCRIPTION OF THE PROCESSING

Some Services provided to the Clients may be sub-contracted to Entities of LEYTON Group which are located in a Third country , and thus imply Transfers of Personal Data collected by Clients which are Data Controllers.

Depending on the character of the Services agreed with the Client, these sub-contracted Services may involve the following processing operations:

- Collection;
- Extraction;
- Retention;
- Recording;
- Use;
- Organisation;
- Structuration;
- Adaptation or modification;
- Alignment or combination;
- Limitation;
- Transfer;
- Consultation;
- Communication by transmission;
- Dissemination or any other form of provision;
- Destruction;

- Deletion.

Article 5.2: PURPOSES

The Processing which requires the Personal Data to be Transferred to Entities located in a Third country pursues all or part of the Purposes that are necessary for the provision of the subscribed Service, which concern the indirect collection (from the initial Processor), then extraction, recording, structuring, analysis and audit of the data, control/ verification, adaptation (and correction, if necessary), dissemination by returning to the Processor and the Data Controller, retention for the time necessary and then destruction after this period, in the context of the Services concerning:

(i) assistance in terms of savings or leveraging the financing generated in particular by means of:

(i.1) the Research and Development Incentive Tax, Tax Credit and the grants and subsidies;
(i.2) the delivery of Certificate of Energy Savings (the "**CEE**") or other white certificates;
(i.3) the optimisation of local and national taxation;
(i.4) the optimisation of corporate taxation;
(i.5) the optimisation of energy taxation;
(i.6) the optimisation of social charges and/or training costs;
(i.7) the optimisation of rental charges;
(i.8) the optimisation of the allocation of the company resources (telecoms, automobile fleet, temporary labour, energy expenses, insurance, etc.)

(ii) the recovery of the daily indemnities of the Clients' employees (the "**IJSS and IJP**"), the payment of the "Transport Payment" contribution (the "**VT**") to which the Clients are subject, the management of declarations of Work-Related Accidents ("**AT**"), of employees' training and peridoc medical check-up organization ("**VM**");
(iii) the provision and the maintenace of software;
(iv) the analysis and monitoring of invoice process and cash recovery.

Article 5.3: CATEGORIES OF PERSONAL DATA

The categories of Personal Data that may be transferred are the following:

a) Identifying information (name, surname, date and place of birth; Social Security Number);
b) Data related to personal life (address, contact details, number of child, marital status, etc.);
c) Data related to professional life (job title, resume, personal number, payroll information, information related to training etc.);
d) Data related to economical and financial life (Tax Identification Number, etc.);

e) Data related to health (information related to accident at work and sick leave, etc.).

Article 5.4: CATEGORIES OF DATA SUBJECTS

The categories of Data Subjects concerned by the Transfer of their Personal Data are the following:
(i) the staff of the Clients (employees, temporary workers, interns, etc.);
(ii) contractual partners of the Clients or their representatives, and their prospective Clients, if any;
(iii) the useful third parties with regard to the Services (particularly, the court officers, court-appointed representatives, etc.).

ARTICLE 6 : OBLIGATIONS OF THE BCR ENTITIES

Article 6.1: COMPLIANCE WITH THESE BCRS

6.1.1. COMPLIANCE BY THE BCR ENTITIES

All of the BCR Entities undertake to rigorously comply with these BCRs, as well as the provisions relating to the Processing of Personal Data, and the security and confidentiality measures contained in the Service Agreements concluded with the Data Controllers.

Any provision resulting from the Data Protection Regulations which may be more strict than the provisions of these BCRs shall prevail.

The BCR Entities undertake to promptly notify to the Data Controller, Thésée, as well as the Supervisory Authority competent for the Data Controller and the Lead Authority competent for the Processor concerning any existing or future obligation imposed by the Data Protection Regulations that :
(i) may prevent a BCR Entity from fulfilling the instructions received from the Data Controller or its obligations under the BCRs or Service Agreement; and/or
(ii) which may have a negative effect on the application of these BCRs.

The Data Controller is entitled to suspend the Transfer of data and/or terminate the contract.

Any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body shall be communicated to the Data Controller unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for the Data Controller and the competent Supervisory Authority for the Processor should be clearly informed about the

request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).

If in specific cases the suspension and/or notification are prohibited, the requested BCR Entity will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested BCR Entity is not in a position to notify the competent Supervisory Authority, general information on the requests received by the Entity must be provided annually to the competent Supervisory Authority (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In any case, Transfers of Personal Data by a BCR Entity to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

For BCR Entities located in the EEA, any judgment of a court or tribunal and any decision of an administrative authority of a Third country requiring a Data Controller or Processor to transfer or disclose Personal Data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting Third country and the Union or a EEA Member State, without prejudice to other grounds for transfer pursuant to Chapter V of GDPR.

6.1.2. OBLIGATIONS OF THE PERSONNEL

6.1.2.1. OBSERVANCE OF THE BCRS AND THE SERVICE AGREEMENTS

All of the BCR Entities shall guarantee that their Personnel authorised to access or process the Data of the Clients shall comply with:
(i) these BCRs, which have been communicated to them in advance;
(ii) the instructions received from the Data Controllers, particularly regarding the security and the confidentiality of the Data and which are contained in the Service Agreements. In this connection, the BCR Entities undertake to communicate to their employees in good time all of the instructions necessary in order to carry out the Processing.

6.1.2.2. COMMITMENTS FOR THE CONFIDENTIALITY AND THE SECURITY OF THE DATA MADE BY THE PERSONNEL

All of the BCR Entities shall ensure that the Personnel authorised to access or process the Data of the Clients are subject to a confidentiality obligation.

Article 6.2: COMMUNICATIONS

The BCR Entities must communicate the complaints and requests of the Data Subjects without undue delay (i) directly to the Data Controller or, (ii) indirectly by the intermediary of the DPO or the Data Exporter.

Article 6.3: SECURITY AND CONFIDENTIALITY OF THE DATA

Considering the current state of knowledge, the costs for implementation and the character, scope, nature, context and the Purposes of the Processing as well as the risks for the rights and freedoms of Data Subjects, for which the degree of probability and seriousness may vary, the BCR Entities shall put in place technical and organisational measures that are appropriate in order to guarantee a level of security for the Data that is adapted to the risk, including, among others, and depending on the needs:

(i) means allowing a guarantee of the constant confidentiality, integrity, availability and resilience of the systems and the processing services;
(ii) means allowing the availability of the Personal Data to be re-established and access to these Personal Data within appropriate timeframes in the case of a physical or technical incident;
(iii) a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the Processing.

A description of the security measures appears in Annex 3.

These measures shall at least meet the requirements of the Data Controller's applicable law and any existing particular measures specified in the Service Agreement signed with the Data Controller.

Article 6.4: PROCEDURE FOR NOTIFICATION IN THE CASE OF A PERSONAL DATA BREACH

The BCR Entities undertake to directly or indirectly by the intermediary of the Data Exporter inform the Data Controllers as soon as possible after they become aware of any Personal Data Breach. In any event, the BCR Entities shall assist the Data Controllers by providing to them all of the useful information in their possession or connected with a Personal Data Breach.

Article 6.5: COMPLIANCE WITH THE INSTRUCTIONS OF THE DATA CONTROLLERS

If a Transfer to a Third country or an international organisation is required by virtue of the law of the European Union or the law of a Member State, the Data Exporter shall, immediately and before the Processing takes place, inform the Data Controller of this unless the law in question prohibits the provision of such information for important reasons of public interest.

The BCR Entities shall only process the Personal Data on behalf of the Data Controllers upon their documented instructions and undertake to comply with these rigorously. If a BCR Entity is unable to comply for any reason whatsoever, it must immediately inform the Data Controller of this either directly or indirectly by the intermediary of the Data Exporter. In such case, the Data Controller may suspend the Transfer of the Data until a solution is found jointly or terminate the contract.

Article 6.6: AID AND ASSISTANCE OF THE DATA CONTROLLERS

6.6.1. OBSERVANCE OF THE DATA PROTECTION REGULATIONS

The BCR Entities shall collect, retain and make available to the Data Controller all of the information necessary for the Data Controller to demonstrate compliance with its obligations provided for by the Data Protection Regulations. The BCR Entities shall assist the Data Controller in replying to investigation or inquiry from Supervisory Authorities.

The BCR Entities and the external Subprocessors undertake to

i) provide, as soon as possible, to the Data Controller all of the information required by an impact analysis as required by Articles 35 et seq. of the GDPR, and which it may not have and which it may be unable to locate itself.

ii) assist the Data Controller in ensuring compliance with the obligations as set out in Articles 32 to 36 of the GDPR taking into account the nature of Processing and information available to the Processor.

iii) facilitate the Data Controller's compliance with the principles of data protection by design and by default

The BCR Entities shall co-operate and assist the Controller to comply with its duty to respect the Data Subject rights and handle their complaints. The BCR Entities shall implement all of the technical and organisational measures necessary in order to assist the Data Controllers, at their request, to update, correct or delete the Data. The BCR Entities and the Subprocessors will execute any necessary measures, when asked by the Data Controller, in order to have the data deleted or anonymised from the moment the identification form is not necessary anymore. The BCR Entities and the Subprocessors will communicate to each Entity to whom the data have been disclosed of any request of rectification, deletion or anonymisation of data.

In addition, the BCR Entity shall immediately inform the Data Controller if in its opinion, an instruction infringes the GDPR or other Union or EEA Member State data protection provisions.

In order to demonstrate compliance with the BCRs, BCR Entities need to maintain a record of all categories of Processing activities carried out on behalf of each Data Controller containing, as per Art. 30.2 GDPR. This record should

be maintained in writing, including in electronic form and should be made available to the Supervisory Authority on request.

6.6.2. REQUESTS BY THE DATA SUBJECTS

The BCR Entities shall transmit any requests by the Data Subjects concerned by the Processing without undue delay and within a maximum of 5 working days, directly to the Data Controllers, or if necessary indirectly by the intermediary of the Data Exporter.

They shall also put in place appropriate technical and organisational measures, to the extent possible, in order to help them respond as soon as possible to these requests, including by communicating any useful information in order to help the Data Controller to comply with the duty to respect the rights of the Data Subjects.

Article 6.7: SUBPROCESSOR

The BCR Entities must comply with the Data Protection Regulations and the provisions contained in the Service Agreements governing the Processing of the Personal Data that they process on behalf of the Data Controllers.

In order to do this, they must:
(i) only sub-contract the Services which involve the Processing of Personal Data after they have received the general or specific consent of the Data Controller;
(ii) if necessary, communicate faithfully and in good time the processing instructions of the Data Controller to the Subprocessor.

The BCR Entity shall obtain the prior informed general written authorization of the Data Controller to appoint a Subprocessor to process Personal Data. The BCR Entity will provide the Data Controller with a comprehensive list of Subprocessors upon Data Controller´s request and will inform the Data Controller of any intended changes concerning the addition or replacement of other Subprocessors so that the Data Controller has the opportunity to object to such changes, or to terminate the contract before the data are communicated to the new Subprocessor.

A BCR Entity may only appoint an external Subprocessor to process Personal Data where a privacy and security risk assessment has been carried out, to determine that this Subprocessor will provide sufficient guarantees that it will implement appropriate technical and organisational measures and complies with applicable EEA Data Protection Regulations.

The BCR Entity must ensure that there is a written contract with the Subprocessor, which is recognised as valid under EEA Data Protection Regulations, and which contains:

- The provisions set out in the Articles 28, 29, 32 of the GDPR ;

- The provisions set out in one of the Articles 45, 46 or 47 of the GDPR ;
- The creation of third-party beneficiary rights for Data Subjects; including the possibility to lodge a complaint before the competent SA and before the courts
- Responsibility towards the Data Controller
- Cooperation duty towards Supervisory Authorities and with the Data Controller
- Data protection safeguards

ARTICLE 7 : LIABILITY

The Data Exporters may be held responsible before the competent Supervisory Authorities and/or before the competent courts by the Data Subject and by the Data Controllers with which they have concluded a Service Agreement for any failings with regard to these BCRs or the Data Protection Regulations that are applicable to them.

The Data Exporter accepts responsibility for and agrees to take the necessary action to remedy the acts of other BCR Entities established outside of EEA or breaches caused by external Subprocessor established outside of EEA and to pay compensation for any damages resulting from a violation of the BCRs.

The Data Exporter will accept liability as if the violation had taken place by him in the EEA Member State in which he is based instead of the BCR Entity outside the EEA or the external Subprocessor established outside of EU. This BCR Entity may not rely on a breach by a Subprocessor (internal or external of the group) of its obligations in order to avoid its own liabilities.

In any event, if an Entity of LEYTON Group is held responsible for a violation of these BCRs committed by a Data Importer, the Data Exporter may request compensation from the BCR Entity who failed to comply with the BCR for any costs, charges, damages, expenses or losses incurred by it.

ARTICLE 8 : RESPONSIBILITY

Article 8.1: RESPONSIBILITY TO DATA CONTROLLER

The Client, acting as Data Controller shall have the right to enforce the BCR against any BCR Entity for breaches they caused.

Moreover, the Client has the right to enforce the BCR against any BCR Entity acting as Data Exporter in case of:

i) a breach of the BCRs or of the Service Agreement by a BCR Entity established outside of EEA

ii) a breach by an external Subprocessor established outside of the EEA to its obligations applicable to as per Article 6.7: .

Article 8.2: RESPONSIBILITY TO THIRD PARTY BENEFICIARIES

The Data Subjects shall be entitled to lodge a complaint before:

- any Supervisory Authority (in particular the Supervisory Authority of the EEA Member State of his/her habitual residence, place of work or place of alleged infringement) and
- the competent court in the EEA (choice for the Data Subject to act before the courts where the Data Controller or Processor has an establishment or where the Data Subject has his or her habitual residence).

In case of a breach by a BCR Entity or an external Subprocessor established outside of the EEA, the Data Subjects may bring their proceedings against the BCR Entity acting as Data Exporter (see ARTICLE 7 : of the present document).

8.2.1. RIGHTS DIRECTLY ENFORCEABLE AGAINST THE PROCESSOR

The Data Subjects can enforce the BCRs as third party beneficiaries directly against the Processor where the requirements at stake are specifically directed to Processors in accordance with the GDPR. In this regard, Data Subjects can enforce the following elements of the BCRs directly against the EEA BCR Entity exporting the data, acting as a Processor:

- Duty to implement appropriate technical and organizational security measures and duty to notify, without undue delay after becoming aware of it, any Personal Data breach to the Client (Article 6.3: and 6.4);
- Duty to respect the instructions from the Client regarding the data processing including for data Transfers to Third countries (Article 6.5:);
- Duty to cooperate with and assist the Data Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Article 6.6:);
- Duty to respect the conditions when engaging a Subprocessor either within or outside the Group (Article 6.7);
- Right to complain through internal complaint mechanisms (Article 10.2:)
- Liability and compensation provisions (Article 7, 8.2.1)
- Jurisdiction provisions (ARTICLE 7 :);
- Easy access to BCRs (Article 9.2:);
- Duty to cooperate with the Supervisory Authority (ARTICLE 12 : 3);
- National legislation preventing respect of BCRs (Article 6.1.1, 6.6.1,16,);
- Third-party beneficiary rights for Data Subjects (Article 8.2:).

8.2.2. RIGHTS ENFORCEABLE AGAINST THE PROCESSOR WHERE THE DATA SUBJECT IS NOT ABLE TO BRING A CLAIM AGAINST THE CLIENT ACTING AS DATA CONTROLLER

The Data Subjects can also enforce, the BCRs as third-party beneficiaries in case the Data Subject is not able to bring a claim against the Client, acting as data Data Controller; because the Client has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Controller by contract of by operation of law, in which case the Data Subject can enforce its rights against such Entity for the following elements:

- Easy access to BCRs for Data Subjects and in particular easy access to the information about third party beneficiary rights for the Data Subject that benefit from them (Article 9.2:)
- The duty to respect the present BCRs (Article 6.1:)
- The existence of a complaint handling process for the BCRs (Article 10.2)
- The creation of third-party beneficiary rights for Data Subjects, including the possibility to lodge a complaint before the competent SA and before the courts (Article 8.2:)
- The burden of proof lies with the BCR Entities (Article 8.3:)
- The liability of the BCR Entities for paying compensation and to remedy breaches of the BCRs (ARTICLE 7 :)
- Duty to cooperate with the Supervisory Authority (ARTICLE 12 : 3)
- Duty to cooperate with the Data Controller (Article 6.6:)
- The duty to respect the data protection principles stated in the present document (Article 6.3: , Article 6.5: Article 6.6: , Article 6.7; Article 6.8)
- Transparency requirements where national legislation prevents the group from complying with the BCRs (Article 6.1.1, 6.6.1, 16)
- The list of entities bound by BCR

The BCR Entity shall be liable for the damage caused by the Processing only where it has not complied with obligations of Data Protection Regulation specifically directed to Processors or where it has acted outside or contrary to lawful instructions of the Client, acting as Data Controller or to the provisions of the BCR (Art. 82.2 GDPR).

Where the BCR Entity and the Client, acting respectively as Processor and Data Controller and involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the Processor (Art. 82.4 GDPR).

Article 8.3: BURDEN OF PROOF

Any harm suffered by a Data Subject or by a Data Controller that is connected with a Transfer of Personal Data carried out in the context of a Service

Agreement is assumed to have been caused by a failure to comply with these BCRs by the Data Importer or an external Subprocessor.

In such a case, the burden of proof is upon the Data Exporter, which must prove that the Data Importer or the external Subprocessor is not responsible for the act which is the source of the harm invoked by this Data Subject or this Data Controller.

ARTICLE 9 : COMMUNICATION OF THE BCRS

Article 9.1: REFERENCE IN SERVICE AGREEMENTS

The BCR Entities shall refer to these BCRs in all of the Service Agreements concluded with the Data Controllers, which shall be indicated by a hypertext link in order to access it by electronic means. The Service Agreement shall mention that BCR Entities will contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller and define the applicable terms and conditions of such audit. Such applicable terms and conditions should not undermine the right of the Data Controller to carry out the audit.

Article 9.2: PROVISION TO THE PUBLIC

As of its definitive approval by the Lead Authority, public version of this document will be made available on the institutional internet site of the Leyton Group and relevant subsidiaries and ensure it is easily accessible by Data Subjects

ARTICLE 10 : GOVERNANCE OF COMPLIANCE

Article 10.2: POINT OF CONTACT

The DPO is the point of contact for all of the BCR Entities and of the Data Subjects, to the email address dpo@leyton.com.

The Data Subject may contact the DPO in order to:

- exercise his rights
- submit a data privacy complaint where the Data Subject considers a breach of the applicable Data Protection Regulations has taken place or there is non-compliance with the BCR.

Where a Data Subject makes a complaint or a request directly to a BCR Entity, the DPO will inform the Data Controller about the complaint or request, as per the procedure defined in Article 6.2: and Article 6.6.2 of the current document.

The DPO will be responsible only for handling those requests according to the Data Controller's instructions. Where the Data Controller has disappeared factually, has ceased to exist or has become insolvent, the DPO will then handle such requests directly, to the extent possible.

Requests and/or complaints must be dealt with without undue delay and in any event within one month after receipt and the DPO shall do all that is necessary in order to address the issue. The period cited above may be extended to two months considering the complexity and the number of requests. The Data Subject must be informed of any delay as well as about the reasons for it.

If the DPO considers that the request or the complaint is not admissible, the DPO will inform the Data Subject within the same delay, of the reasons for not taking action and on the possibility of lodging a complaint with the competent Supervisory Authority and lodging a claim before the court.

The Data Subjects shall in any event retain the right to raise a claim before a Supervisory Authority or the competent courts.

The DPO shall also manage the requests by the Supervisory Authorities so that they are more effectively managed within the BCR Entities.

ARTICLE 11 : MODIFICATION OF THE BCRS

At the initiative of the DPO, with the consent of the Board of Directors of Thésée, or at the initiative of the latter, these BCRs may be modified in order to take into account notably:

(i) the modifications and/or developments of the Data Protection Regulations;
(ii) the modifications of the structure of the Leyton Group.

Such modifications to the BCRs or to the list of BCR Entities shall be documented and archived; former versions should be saved digitally.

In such a case, the modifications shall become enforceable with regard to the BCR Entities upon prior notification of the BCR Entities and once the changes have been reported to all BCR Entities and the relevant Supervisory Authorities via the competent Supervisory Authorities, and the new version has been made available to the Data Subjects, the Data Controllers and employees.

The modifications of the BCRs shall systematically be brought to the knowledge of all of the LEYTON Group entities, the relevant Supervisory Authorities via the CNIL and the Data Controllers by the DPO as soon as possible.

Where a change affects the Processing conditions, the information should be given to the Data Controller in such a timely fashion that the Data Controller

has the possibility to object to the change or to terminate the contract before the modification is made (for instance, on any intended changes concerning the addition or replacement of Subprocessors, before the data are communicated to the new Subprocessor).

ARTICLE 12 : COOPERATION WITH THE SUPERVISORY AUTHORITIES

The Supervisory Authorities may also themselves carry out audits with regard to the protection of data by each BCR Entity. In case observations result from the Supervisory Authorities' audit, the BCR Entities will take into account such observations and implement corrective action when requested.

Each BCR Entity undertakes to cooperate with the Supervisory Authorities competent for the Data Controllers for whom they process the Data in their name and on their behalf. The Supervisory Authorities may carry out verifications of each BCR Entity. The BCR Entities take into account Supervisory Authorities' advice and comply with their decisions, without any limitation.

ARTICLE 13 : THE TOOLS FOR CONFORMITY

In order to assist the Personnel of the BCR Entities to apply these BCRs and the rules resulting from the Regulations, the supporting policies will be implemented regarding :
(i) Retention of data and archiving system;
(ii) A Management of Personal Data Breach;"
(iii) Management of the right of Data Subject;"
(iv) Protection of Data
(v) The Use of information and communications systems.

ANNEX 1: LIST AND PRESENTATION OF THE ENTITIES UNDERTAKING TO OBSERVE THE BCRS

Leyton is a large international consulting firm dedicated to improving the overall performance of its clients by using one of their three business lines: financial innovation, consulting and outsourced Services. Leyton Group operates in 12 countries including: 8 countries within the EEA (France, Belgium, Spain, Portugal, Italy, Germany, Poland, Sweden and Netherlands), 2 secure Third countries (United Kingdom, Canada) and 1 Third country (Morocco).

THESEE
16 Boulevard Garibaldi
92130 Issy les Moulineaux
Registration number: 491828554

Thésée is the holding company of Leyton Group.

LEYTON FRANCE
16 Boulevard Garibaldi
92130 Issy les Moulineaux
Registration number: 504868399

Leyton France is a services company that processes data for all or part of the Purposes described in the part 5.2 of this document Its Clients are solely professional, companies and public entities.

LEYTON CTR
16 Boulevard Garibaldi
92130 Issy les Moulineaux
Registration number: 414600270

LEYTON CTR is a services company that processes data for all or part of the Purposes described in the part 5.2 of this document. Its Clients are solely professional, companies and public entities.

OAP
16 Boulevard Garibaldi
92130 Issy les Moulineaux
Registration number : 523311058

OAP is a services company that processes data for all or part of the following Purpose(s):

- the optimisation of the allocation of the company resources (telecoms, automobile fleet, temporary labour, energy expenses, etc.)
- the optimisation of rental charges
- the analysis and monitoring of invoice process and cash recovery

Its Clients are solely professional, companies and public entities.

OFEE
16 Boulevard Garibaldi
92130 Issy les Moulineaux
Registration number: 504668377

OFEE is a services company that processes data for all or part of the following Purpose(s):

- the delivery of Certificate of Energy Savings (the "CEE") and other white certificates;
- the optimisation of energy taxation;
- the optimisation of the allocation of the company resources (energy expenses)

Its Clients are solely professional, companies and public entities.

LEYTON RISK MANAGEMENT
16 Boulevard Garibaldi
92130 Issy les Moulineaux
Registration number: 423812254

Leyton Risk Management is a services company that processes data for all or part of the following Purpose(s): the optimisation of the allocation of the company resources (insurance costs). Its Clients are solely professional, companies and public entities.

LEYTON JUDO
16 Boulevard Garibaldi
92130 Issy les Moulineaux
Registration number : 879286003

LEYTON BENELUX
Chaussée de la Hulpe 166
1170 Brussels
Registration number: BE0811.483.88

Leyton Belgium is a services company that processes data for all or part of the following Purpose(s):

- the Research and Development Incentive Tax, Tax Credit and the aids and subsidies;
- the optimisation of social contributions.

Its Clients are solely professional, companies and public entities.

LEYTON NETHERLANDS
Secoya Papendorpseweg 99
3528 BJ Utrecht

Leyton Netherlands is a services company that processes data for all or part of the following Purpose(s):

- the Research and Development Incentive Tax, Tax Credit and the aids and subsidies;
- the optimisation of social contributions.

Its Clients are solely professional, companies and public entities.

LEYTON IBERIA
Plaza Xavier Cugat 2, Edificio D, 4 Planta
08017 Sant Cugat del Vallés, Barcelona.
Registration number: B-66286188

Leyton IBERIA is a services company that processes data for all or part of the following Purposes:

- the Research and Development Incentive Tax, Tax Credit and the aids and subsidies;
- the optimisation of local and national taxation;
- the optimisation of social contributions.

Its Clients are solely professional and companies.

THESEE PORTUGAL
R. Daciano Baptista Marques, 245. Lake Towers – Edificio D
4400-617 Vila Nova de Gaia (Porto)

Thésée Portugal is a services company that processes data for all or part of the following Purposes:

- the Research and Development Incentive Tax, Tax Credit and the aids and subsidies;
- the optimisation of local and national taxation;
- the optimisation of social contributions.

Its Clients are solely professional and companies.

LEYTON ITALIA
Via Melchiorre Gioia 26
20124 Milano
Registration number : REA MI 2119395

Leyton Italia is a services company that processes data for all or part of the following Purpose(s):

- the Research and Development Incentive Tax, Tax Credit and the aids and subsidies;
- the delivery of Certificate of Energy Savings (the “CEE”) and other white certificates;
- the optimisation of energy taxation;
- the optimisation of the allocation of the company resources (energy expenses)

- the optimisation of local and national taxation;

Its Clients are solely professional, companies and public entities.

OFEE ITALIA
Via Melchiorre Gioia 26
20124 Milano
Registration number : REA MI 2534436

OFEE Italia is a services company that processes data for all or part of the following Purpose(s):

- the delivery of Certificate of Energy Savings (the "CEE") and other white certificates;
- the optimisation of energy taxation;
- the optimisation of the allocation of the company resources (energy expenses)

Its Clients are solely professional, companies and public entities.

LEYTON POLAND
Wspólna 70
00-687 Warszawa
Registration number: KRS 0000739425

Leyton Poland is a services company that processes data for all or part of the following Purpose(s): the Research and Development Incentive Tax, Tax Credit and the aids and subsidies. Its Clients are solely professional, companies and public entities.

LEYTON GERMANY
Bleichstraße 20
40211 Düsseldorf - Germany
Registration number: HRB: 89458

Leyton Germany is a services company that processes data for all or part of the following Purpose(s): the Research and Development Incentive Tax, Tax Credit and the aids and subsidies. Its Clients are solely professional, companies and public entities.

LEYTON SWEDEN
Klarabergsviadukten 63,
111 64 Stockholm, Suède
Registration number: 559272 – 2663

Leyton Sweden is a services company that processes data for all or part of the following Purpose(s): the Research and Development Incentive Tax, Tax Credit and the aids and subsidies. Its Clients are solely professional, companies and public entities.

LEYTON MAROC
Plateau 502, 5ème étage Park Shore
14 Parc Casanearshore Sidi Maârouf Casablanca
Registration Number: 165799

Leyton Maroc is a services company acting as a Sub-processor that provides internal support Services to the subsidiaries of Leyton Group for all or part of the Purposes described above (§ "Anticipated purposes of data Transfers for processing activities"). Its clients are solely the entities of Leyton Group.

THESEE MAROC
Plateau 502, 5ème étage Park Shore
14 Parc Casanearshore Sidi Maârouf Casablanca
Registration number: 245533

Thésée Maroc is a services company acting as a Sub-processor that provides internal support Services to the subsidiaries of Leyton Group for all or part of the Purposes described above (§ "Anticipated purposes of data Transfers for processing activities"). Its Clients are solely the entities of Leyton Group.

THESEE CANADA
1260 Boulevard Robert Bourassa
Montreal, Quebec H3B 3B9
Registration number: 1165640989

Thésée Canada is the holding company of Leyton Finder Expert.

LEYTON FINDER EXPERT
1260 Boulevard Robert Bourassa
Montreal, Quebec H3B 3B9
Registration number: 1146449062

Leyton Finder Expert is a services company that processes data for all or part of the following Purpose(s): the Research and Development Incentive Tax, Tax Credit and the aids and subsidies. Its clients are solely professional, companies and public entities.

LEYTON UNITED KINGDOM
Harmsworth House
13-15 Bouverie Street
EC4Y 8DP, London
Registration Number : 980788660

Leyton United Kingdom is a services company that processes data for all or part of the following purpose(s) :

- the Research and Development Incentive Tax, Tax Credit and the aids and subsidies;
- the optimisation of social contributions

- the delivery of Certificate of Energy Savings (the “CEE”) and other white certificates;
- the optimisation of energy taxation;
- the optimisation of the allocation of the company resources (energy expenses)

Its clients are solely professional, companies and public entities.

ANNEX 2: GDPR ARTICLES REFERRED IN THE BCR

ART. 28. GDPR PROCESSOR

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

    1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

    2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

    3. takes all measures required pursuant to Article 32;

    4. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

    5. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond

to requests for exercising the data subject's rights laid down in Chapter III;

6. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

7. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

8. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

ART. 29 GDPR PROCESSING UNDER THE AUTHORITY OF THE CONTROLLER OR PROCESSOR

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

ART. 30 GDPR RECORDS OF PROCESSING ACTIVITIES

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. [2]That record shall contain all of the following information:

    1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

    2. the purposes of the processing;

    3. a description of the categories of data subjects and of the categories of personal data;

    4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

    5. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third

country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

6. where possible, the envisaged time limits for erasure of the different categories of data;

7. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

    1. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

    2. the categories of processing carried out on behalf of each controller;

    3. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

    4. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

ART. 32 GDPR SECURITY OF PROCESSING

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    1. the pseudonymisation and encryption of personal data;

    2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

ART. 33 GDPR NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural

persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

    1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

    3. describe the likely consequences of the personal data breach;

    4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

ART. 34 GDPR COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

    1. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

    2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

    3. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

ART. 35 GDPR DATA PROTECTION IMPACT ASSESSMENT

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

    1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

2. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

3. a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

    1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

    2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

    3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

    4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

ART. 36 GDPR PRIOR CONSULTATION

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

    1. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

2. the purposes and means of the intended processing;

3. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

4. where applicable, the contact details of the data protection officer;

5. the data protection impact assessment provided for in Article 35; and

6. any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

ART. 37 GDPR DESIGNATION OF THE DATA PROTECTION OFFICER

1. The controller and the processor shall designate a data protection officer in any case where:

    1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

    2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

    3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

ART. 45 GDPR TRANSFERS ON THE BASIS OF AN ADEQUACY DECISION

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

    1. the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

2. the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

3. the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).
On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

ART. 46 GDPR TRANSFERS SUBJECT TO APPROPRIATE SAFEGUARDS

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

    1. a legally binding and enforceable instrument between public authorities or bodies;

    2. binding corporate rules in accordance with Article 47;

    3. standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

    4. standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

    5. an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

6. an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

    1. contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

    2. provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

ART. 47 GDPR BINDING CORPORATE RULES

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

    1. are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

    2. expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

    3. fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

1. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

2. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

3. their legally binding nature, both internally and externally;

4. the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

5. the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

6. the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

7. how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

8. the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

9. the complaint procedures;

10. the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

11. the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

12. the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

13. the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

14. the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

ART. 49 GDPR DEROGATIONS FOR SPECIFIC SITUATIONS

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

    1. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for

the data subject due to the absence of an adequacy decision and appropriate safeguards;

2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

4. the transfer is necessary for important reasons of public interest;

5. the transfer is necessary for the establishment, exercise or defence of legal claims;

6. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

7. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

ART. 82 GDPR RIGHT TO COMPENSATION AND LIABILITY

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

ANNEX 3: DESCRIPTION OF SECURITY MEASURES

1– PHYSICAL SECURITY

- Access badges with logs or security agent

2- ACCESS MANAGEMENT

- Annual review of access rights
- Logs of GPO changes
- Logs of file and folder access permissions owners

3– DATA HOSTING

- Data centres located in France and certified in certified ISO 27001, SOC 2 Part II

4 – NETWORK SECURITY

- Intrusion prevention system with automatic alert (IPS)
- Malware protection
- Firewall and SSL inspection
- Application control
- Antivirus EDR
- SOC

5 – NETWORK REPORTING

- Traffic log, event log, or security log information
- Tracks of logon / logout and user activity
- Monitoring of critical applications such as Active Directory, SQL or internal application

6 – COMPUTER SECURISATION

- Strong password policy with regular change
- Automatic lock in case of prolonged inactivity
- Secured remote access process
- drive eraser solution for laptop scrap

7 – EXCHANGES SECURITY

- VPN SSL
- WIFI WPA 2
- E-mails encrypted in TLS 1.2
- Anti-spam
- DKIM and DMARC

8 – EMPLOYEE SENSIBILISATION

- Use of shredders
- Clean desk policy

- Charter of use of information system
- Internal policies
- Data protection and security training programs