BINDING CORPORATE RULES FOR PROCESSORS (OR BCR-P)

TALAN as a Processor

I. INTRODUCTION

1. Purpose

Talan has adopted Binding Corporate Rules in order to ensure the highest level of protection of the data processed by Talan. These Binding Corporate Rules are intended to introduce data protection principles and procedures that each Talan Entity is committed to comply with to ensure a high level of protection for Personal Data within Talan.

2. Scope of the BCRs

a) Geographical scope

These BCRs cover all Personal Data transferred and processed between the Talan Entities in the course of Talan's activities as a Processor, regardless of the origin of such Personal Data.

In practice, this means that BCRs will apply to Personal Data transferred from :

- An EEA Talan Entity to another EEA Talan Entity;
- An EEA Talan Entity to a non-EEA Talan Entity;
- A non-EEA Talan Entity to an EEA Talan Entity;
- A non-EEA Talan Entity to another non-EEA Talan Entity.

The Talan Entities are listed in **Appendix 1** of the BCRs.

b) Material scope

The BCRs apply to the Processing of Personal Data by the Talan Group acting as a Processor, following the instructions of its Clients, Data Controllers, regardless of the nature or category of the Data Subject or Personal Data. A general description of the material scope of the BCRs is provided in **Appendix 2** of these BCRs.

3. Binding nature of the BCRs

Each Talan Entity, including its Employees, is required to comply with the Binding Corporate Rules.

a) With respect to Talan Entities

In practice, the Intra-Group Agreement has been entered into between TALAN CORPORATE and each Talan Entity listed in **Appendix 1** of these BCRs.

By executing the Intra-Group Agreement, each Talan Entity has agreed to be fully bound by the provisions of the BCRs and to comply with and implement them within its own organization.

b) With respect to Employees

The BCRs are part of the Group's internal policies through the Talan Code of Conduct, which provides that the Employees of each Talan Entity are subject to the provisions of the BCRs.

In this respect, whenever necessary, or at any time, Employees of each of the Talan Entities may contact the Talan Group DPO (dpo@talan.com) for assistance or information on compliance with the rules on the protection of Personal Data.

Talan's Code of Conduct reminds Employees of each Talan Entity that any breach of the rules and safety measures concerning compliance with the Applicable Law or Talan Group rules, in particular the BCRs, is likely to engage the responsibility of the Employee and lead to warnings or even disciplinary sanctions proportionate to the seriousness of the facts concerned. In the latter case, the procedures provided for in the internal regulations and local legislation will be applied.

Talan's Code of Conduct also provides that Talan reserves the right to initiate or cause to be initiated criminal proceedings independently of any disciplinary action taken, including for violations of the Applicable Law.

In addition, as detailed in Article III.4 of these BCRs, the Employees of each Talan Entity are informed of the provisions of the BCRs and the obligations arising therefrom through internal announcements and training programs covering the implementation of the BCRs.

c) With respect to Talan's Clients

When Talan acts as a Processor, it undertakes to enter into Service Agreements that comply with the requirements of Article 28 of the GDPR.

In addition, Talan agrees to comply with the BCRs that will be made binding on Talan Entities to a Data Controller with a specific reference in the Service Agreement.

In any event, a Data Controller may enforce the BCRs against any Talan Entity for violations of the BCRs caused by it, in accordance with the provisions set forth in Article IV.3.b).

II. DEFINITIONS AND PRINCIPLES OF DATA PROTECTION

1. Definitions

The terms and expressions used in the BCRs are defined as follows and shall be interpreted, in all circumstances, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

"Intra-Group Agreement" means the legally binding agreement which purpose is to make the BCRs binding on the Talan Entities.

"Data Protection Impact Assessment" or **"DPIA"** means a process to describe the Processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of Data Subjects resulting from the Processing of Personal Data by evaluating them and determining measures to address them.

"Supervisory Authority(ies)" or **"Data Protection Authority(ies)"** means the EU independent public authorities responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to Processing and to facilitate the free flow of personal data within the EU.

"EU Standard contractual clauses (SCCs)" means the European Commission's Standard Clauses for the transfer of personal data from EU to third countries as set out in the Annex to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021.

"Sensitive Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

"Client(s)" or "Data Controller" means any natural or legal person to whom Talan provides services, pursuant to a Service Agreement and who, alone or jointly with others, determines the purposes and means of the Processing.

"Service Agreement" means a written agreement between a Data Controller and a Processor, pursuant to which the Processor provides services to the Data Controller and which involves the Processing of Personal Data by the Processor in accordance with the instructions of the Data Controller.

"Data Protection Officer" or **"DPO"** means the designated Employees with expert knowledge of data protection law and practice, dedicated to advising, informing and monitoring compliance with the Applicable Law, and who are part of the Data Protection Officer network described in Article IV. 1.

"Local DPO" means an Employee working for a Talan Entity whose function is to monitor that Employees are aware of and comply with the Applicable Law and Talan's policies, procedures and guidelines relating thereto, and in particular the BCRs.

"Talan Group DPO" means the person responsible at the Talan Group level for ensuring that Talan Entities and their Employees are aware of and comply with the Applicable Law and Talan's policies, procedures and guidelines relating to the protection of Personal Data, and in particular the BCRs.

"Recipient(s)" means the natural or legal person, public authority, department or other body that receives Personal Data, whether or not it is a third party; however, authorities that may receive Personal Data in the context of a particular investigation mission in accordance with EU law or the law of a Member State are not considered Recipients.

"Personal Data" means any information relating to an identified or identifiable natural person (i.e., the "**Data Subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Employee" means any current, former or future member of Talan's staff, including temporary workers and interns.

"Talan Entity(ies)" means any Group entity that has ratified the Intra-Group Agreement and is therefore bound by the BCRs.

"EEA Talan Entity(ies)" means any Talan Entity located in the European Economic Area (or **"EEA"**).

"Non-EEA Talan Entity(ies)" means any Talan Entity located outside the EEA.

"Exporting EEA Talan Entity" means the Talan Entity, located within the EEA, that transfers Personal Data outside the EEA.

"Applicable Law" means any applicable Personal Data protection regulations that may apply and in particular (i) the GDPR and (ii) any national laws and regulations applicable to the Processing of Personal Data it being specified that the GDPR prevails over national laws and regulations, except where the latter are more protective.

"Data Subject(s)" means any identified or identifiable natural person whose Personal Data is processed. Data Subjects are third party beneficiaries with respect to the Transfer of their Personal Data.

"Binding Corporate Rules" or **"BCRs"** or **"BCR-P"** means a data protection policy adhered to by a Processor for Transfers or a set of Transfers of Personal Data to a sub-processor in one or more third countries within a group of companies, or a group of companies engaged in a common economic activity. For the Talan Group, the BCRs constitute the present document and its appendixes.

"General Data Protection Regulation" or **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regards to the processing of personal data and the free movement of such data.

"Processor" means the natural or legal person, public authority, department or other body that processes Personal Data on behalf of the Data Controller.

"Talan", **"Group"** or **"Talan Group"** means all entities owned and/or controlled directly or indirectly by TALAN CORPORATE.

"Processing" covers a wide range of operations performed on Personal Data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

"**Transfer(s)"** means disclosure, transmission or process of making Personal Data available to any third party.

"Personal Data Breach" means the destruction, loss, alteration, unauthorized disclosure of, or accidental or unlawful access to Personal Data transmitted, stored or otherwise processed, whether or not resulting from a breach of security.

"**BCR Lead**" means the competent Supervisory Authority in the context of the BCRs approval procedure (i.e. the French Supervisory Authority, the "CNIL").

2. Talan's Data Protection Principles

Each Talan Entity agrees to comply with the data protection principles set forth in these BCRs as follows, regardless of the Applicable Law, unless the Applicable Law provides for more stringent requirements than those set forth in the BCRs. All of these principles are promoted and implemented within each Talan Entity through a set of policies and training on the protection of Personal Data.

a) Transparency, fairness and lawfulness

Each Talan Entity undertakes to be transparent regarding its Processing activities and has a general duty to help and assist the Data Controller to comply with the Applicable Law.
Talan Entities will provide Data Controller with reasonable cooperation and assistance within a reasonable period of time to help facilitate their respective obligations under Applicable Law, to the extent Data Controller, in its use of the services, does not have the reasonable ability to address such obligations. This may include, for example, a responsibility to comply with certain instructions stipulated in the contract or other legally binding document with a Data Controller, such as assisting the Data Controller in complying with the requirement to inform and explain to Data Subjects how their Personal Data will be Processed at the time their Personal Data is collected.

b) Purpose limitation

Each Talan Entity has a duty to process the Personal Data only on behalf of the Data Controller and in compliance with its documented instructions, including with respect to Transfers of Personal Data to a third country, unless it is required to do so by Union or Member State law to which it is subject. In such case, the relevant Talan Entity shall inform the Data Controller of that legal requirement prior to the Processing takes place, unless the relevant law prohibits such information on important grounds of public interest (Article 28 3) a. of the GDPR). In other cases, if a Talan Entity cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the Transfer of Personal Data and/or terminate the Service Agreement.

On the termination of the provision of services related to the Personal Data Processing, the relevant Talan Entity shall, at the choice of the Data Controller, delete or return all the Personal Data transferred to the Data Controller and delete the copies thereof and certify to the Data Controller that it has done so, unless legislation imposed upon them requires storage of the Personal Data transferred. In that case, the relevant Talan Entity shall inform the Data Controller and warrant that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

c) Data quality

Each Talan Entity has a general obligation to help and assist the Data Controller to comply with the law, notably:

- Each Talan Entity will execute any necessary measures when asked by the Data Controller, in order to have the data updated, corrected or deleted. Each Talan Entity will inform each Talan Entity member to whom the data have been disclosed of any rectification, or deletion of data;

- Each Talan Entity will execute any necessary measures, when asked by the Data Controller, in order to have the data deleted or anonymized from the moment the identification form is not necessary anymore. Each Talan Entity will communicate to each entity to whom the data have been disclosed of any deletion or anonymization of data.

d) Security

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, each Talan Entity will have a duty to implement all appropriate technical

and organizational measures to ensure a level of security appropriate to the risks presented by the Processing, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

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.

The Data Controller and the Talan Entities shall take steps to ensure that any natural person acting under the authority of the Data Controller or the Talan Entities who has access to Personal Data does not process them except on instructions from the Data Controller, unless he or she is required to do so by the Applicable Law.

Each Talan Entity will also have a duty to assist the Data Controller in ensuring compliance with the obligations to notify the competent Supervisory Authority and Data Subjects where applicable in case of Personal Data Breach, to conduct a DPIA and to consult the competent Supervisory Authority prior to Processing where required as set out in Articles 32 to 36 of the GDPR taking into account the nature of Processing and information available to each Talan Entity (Article 28 3) f. of the GDPR).

Each Talan Entity must implement technical and organizational measures which at least meet the requirements of the Data Controller's applicable law and any existing particular measures specified in the Service Agreement.

Talan Entities shall inform the Data Controller without undue delay after becoming aware of any Personal Data Breach. In addition, any Talan Entity acting as a sub-processor shall have the duty to inform the Talan Entity acting as the main processor and the Data Controller without undue delay after becoming aware of any Personal Data Breach.

e) Data Subjects' rights

Each Talan Entity shall execute any appropriate technical and organizational measures, insofar as this is possible, when asked by the Data Controller, for the fulfilment of the Data Controller's obligations to respond to requests for exercising Data Subjects' rights as set out in Chapter III of the GDPR (Article 28 3) e. of the GDPR) such as the right to be informed, the right to access to Personal Data, the rights to rectification and erasure, the right to portability, the right to object and the right not to be subject to a decision based solely on automated processing. Talan Entities shall communicate any useful information in order to help the Data Controller to comply with the duty to respect the rights of the data subjects. Each Talan Entity will transmit to the Data Controller any Data Subject request without answering it unless he is authorized to do so.

Appendix 4 and Article III. 2 of these BCRs describe the procedure for handling Data Subject requests to be followed by Talan Entities.

f) Sub-processing within the Group

Personal Data may be sub-processed to other Talan Entities only with the prior informed specific or general prior written authorization of the Data Controller. The Service Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new sub-processor. If a general authorization is given, the Data Controller should be informed by the Talan Entity acting as a main processor of any intended changes concerning the addition or replacement of a Talan Entity acting as a sub-processor sufficiently in advance so that the Data Controller has the possibility to object to the change or terminate the Service Agreement before the Personal Data are communicated to the new Talan Entity acting as a sub-processor.

g) Onward transfers to external sub-processors

Personal Data may be sub-processed by non-members of the BCRs only with the prior informed specific or general written authorization of the Data Controller. If general authorization is given, the Data Controller should be informed by the relevant Talan Entity of any intended changes concerning the addition or replacement of sub-processors sufficiently in advance so that the Data Controller has the possibility to object to the change or terminate the Service Agreement before the Personal Data are communicated to the new sub-processors.

Where the Talan Entity subcontracts its obligations under the Service Agreement, with the authorization of the Data Controller, it shall do so only by way of a contract or other legal act under Union or State law concluded with the sub-processor which provides adequate protection as set out in Articles 28, 29, 32, 45, 46 and 47 of the GDPR and ensures that the same data protection obligations as set out in the Service Agreement between the Data Controller and the relevant Talan Entity as well as Articles I.3, II.2, IV.2, IV.4. a), IV.6, IV.7, V.1, V.2, V.3 of these BCRs are imposed on the sub-processor, in particular providing sufficient guarantees to implement technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR (Article 28 4) of the GDPR).

III. EFFECTIVENESS OF THE BCRs

1. Access to the BCRs by Data Subjects

Data Subjects have the right to easy access to BCRs. Consequently, Talan undertakes to ensure that Data Subjects benefiting from third party beneficiary rights are provided with information about their third party beneficiary rights with respect to the Processing of their Personal Data and the means of exercising such rights.

For this purpose, essential commitments taken under these BCRs with respect to Data Subjects will be included in a public version of the BCRs that will be published on the Talan Group's website www.talan.com in a way that is easily accessible to Data Subjects.

These commitments that will be included in the public version of the BCRs are:

- **The duty to respect the BCR**: Article I.3. “Binding nature of the BCRs”;
- **Third party beneficiary rights**: Article IV.2. “Third party beneficiary rights”;
- **Liability towards the Data Controller**: Article IV.3 b) “Liability towards the Data Controller”;
- **Sufficient financial resources to cover compensation for the violation of the BCRs**: Article IV.3 a) “Liability towards third party beneficiaries” and b) “Liability towards the Data Controller”;

- **The burden of proof lies with the company not the individual**: Article IV.3 c) ”The burden of proof”;
- **The duty to maintain a record of all categories of Processing activities and implement Privacy by Design and by Default**: Articles IV. 4 a) “Record” and b) “Privacy by Design and by Default”;
- **The existence of a complaint handling process for the BCRs**: Article III. 2 “Internal complaint mechanisms” and **Appendix 4** “Procedure for handling Data Subject requests”;
- **The duty to cooperate with Supervisory Authorities**: Article IV. 6 “Cooperation with Supervisory Authorities”;
- **The duty to cooperate with the Controller**: Article IV. 7 ”Cooperation with the Data Controller”;
- **A description of the transfers and material scope covered by the BCRs**: Article I. 2 b) ”Material scope” and **Appendix 2** ”General description of the BCRs’ material scope”;
- **A statement of the geographical scope of the BCRs**: Article I. 2 a) ”Geographical scope” and **Appendix 1** “List of Talan Entities bound by the BCRs”;
- **A description of the privacy principles including the rules on transfers or onward transfers outside of the EU**: Article II. 2. ”Talan's Data Protection Principles”;
- **The list of entities bound by BCRs**: **Appendix 1** “List of Talan Entities bound by the BCRs”;
- **The need to be transparent where national legislation prevents the group from complying with the BCRs**: Article V. 3 ”Actions in case of national legislation preventing respect of the BCRs” and **Appendix 7** ”Competent Authority Control Management Policies”.

In addition, the list of Talan Entities is published on the Talan Group's website in a way that is easily accessible to Data Subjects.

2. Internal complaint mechanisms

Each Talan Entity shall promptly transmit any complaint or request from a Data Subject that it receives to the Data Controller. The relevant Talan Entity shall await instructions from the Data Controller on how to proceed, unless otherwise agreed between the parties in the Service Agreement.

Although Talan encourages Data Subjects to contact the Data Controller directly, Talan still allows them to submit complaint or request through the following dedicated procedure for handling Data Subject requests described in **Appendix 4**:

- Main Procedure:

  - Talan identifies the Client or partner acting as the Data Controller in the request and transfers the complaint or request to the contractually identified Data Controller's contact point or, in the absence of such contact point, to an active and qualified Data Controller contact.
  - Talan shall use all reasonable means at its disposal to assist the Data Controller in complying with the Data Subject's complaint or request.

If contractually provided for, the Data Controller may ask Talan to respond directly to the Data Subject's complaint or request. In this case, Talan shall immediately contact the Talan Group DPO to assist it in responding to the Data Subject in a proper manner.

- Procedure when the Data Controller has disappeared:

In accordance with the commitments described in these BCRs, the Talan Group, and therefore by extension each of its Employees, shall use all possible and reasonable means to comply with a Data Subject's complaint or request when it is materially impossible for the Data Subject to make such a complaint or request to the Data Controller.

Specifically, a Data Subject may assert certain rights under the BCRs, if:

- The Data Subject is not able to lodge a complaint against the Data Controller or make a request because the Data Controller has materially disappeared, ceased to exist in law, and
- The Data Controller's legal obligations have not been transferred in their entirety, by contract or by operation of law, to another successor entity to which the Data Subject can assert their rights, and
- The Data Subject may demonstrate that he or she has suffered damages and that these damages are likely to have resulted from a breach of the BCRs.

When a Talan Entity receives such a complaint or request, it immediately refers it to the Talan Group DPO, in accordance with Talan's procedure for handling Data Subject requests.

Upon receipt of a complaint or request, the Talan Group DPO may, in case or reasonable doubt, proceed to verification of the identity of the Data Subject.

The Talan Group DPO will inform the Data Subject of their rights and the modalities for the exercise of those rights by sending a specific information notice including the following indications:

- The Talan Group DPO is the contact point to which the complaint or request should be sent by electronic means at dpo@talan.com;
- Complaint or request shall be dealt without undue delay and in any event within one month by the Talan Group DPO. Taking into account the complexity and number of the complaints or requests, that period may be extended by two further months at the utmost, in which case the Data Subject should be informed accordingly, without undue delay and in any event within one month by the Talan Group DPO, together with the reasons for the delay;
- If the complaint or request is rejected as unjustified, the Talan Group DPO will send to the Data Subject a refusal notice;
- If the complaint or request is found justified, the Talan Group DPO will access the complaint or request;
- If the Data Subject is not satisfied with the Talan Group DPO's answer, he or she has a right to lodge a complaint before the competent Supervisory Authority and/or the competent courts;
- If the Talan Group DPO does not take action on the complaint or request within due time, the Data Subject has a right to lodge a complaint before the competent Supervisory Authority and/or the competent courts.

In addition to recording the request, the Talan Group DPO will complete and keep a summary form of the request.

3. Security and privacy

The protection of Personal Data against data breaches is one of Talan's priorities. Therefore:

i. Each Talan Entity is required to process Personal Data on behalf of the Data Controller only, in compliance with its instructions and the security and confidentiality measures set forth in the Service Agreement.
ii. Each Employee is required to process Personal Data on behalf of the Data Controller only, in compliance with its instructions and the security and confidentiality measures set forth in the Service Agreement.
iii. Each Talan Entity must implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, accidental loss, alteration, unauthorized dissemination or access, in particular when the Processing involves data transmissions in a network, as well as against any other form of unlawful Processing. These

measures must ensure, taking into account the state of the art and the costs associated with their implementation, a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected.

Therefore, Talan shall ensure the security of the information through the implementation of appropriate policies and procedures within the Talan Group, setting out all physical and logical measures necessary to prevent the inadvertent destruction or modification of Personal Data, or any unauthorized disclosure or access. These policies and procedures shall be subject to regular audits in accordance with Article III.5.

Sensitive Data must be subject to specific, enhanced security measures.

Access to Personal Data is limited to Recipients only to the extent necessary to perform their job duties. Employees who fail to comply with applicable information security policies and procedures may be subject to disciplinary action.

4. Training program

Appropriate training about the BCRs shall be provided to Employees who have permanent or regular access to Personal Data and who are associated with the collection of Personal Data or the development of tools used to process Personal Data.

In this regard, Talan has created and implemented a mandatory and up to date Employee Data Protection Training Program to be completed every two years.

The purpose of this training program is to ensure that all Employees are aware of and understand the data protection key principles and requirements as well as the purpose and content of these BCRs.

The Employees receive customized training appropriate to their duties and responsibilities within Talan to enable them to process Personal Data in accordance with the principles of the BCRs.

This training program covers, in particular but not exclusively, the procedure for handling legally binding request for disclosure of Personal Data by a law enforcement authority or state security body and includes a mandatory BCRs questionnaire for all Employees of Talan Entities. The completion and success rate of this questionnaire is monitored by the manager of the Employee concerned and globally by the Talan Group DPO.

In addition, the Talan Group DPO or Local DPOs may provide training program to the Employees irrespective of the above mentioned training program, whenever they consider it necessary, in particular but not exclusively, following a data breach or in the event of change in Applicable Law.

5. Audit

The Group is required to have data protection audits conducted, on regular basis or at the specific request of the Talan Group DPO, by the Talan Audit Department or external accredited auditors to ensure the verification of compliance with the BCRs.

In this respect, Talan has defined internal policies relating to (i) the existence of an audit program covering all aspects of the BCRs including methods to ensure the implementation of corrective measures, (ii) the management of controls by competent authorities providing for the terms and conditions under which the audits required by BCRs will be conducted.

These internal policies are described in **Appendix 5**.

These internal audit policies cover all aspects of the BCRs, including methods to ensure the implementation of corrective measures and are applicable to all Talan Entities.

Annual BCRs audit

Talan's internal policy on auditing compliance with the BCRs provides for a thorough yearly control of the Talan Entities' compliance with the engagements set forth in the Talan Group's BCRs.

The audit results are communicated in a report to the Talan Group DPO, the local DPO, the Talan Group management and the management of the Talan Entities concerned. They are also made available to the Data Controllers.

Audit at the request of a Data Controller

As a Processor, each Talan Entity agrees to be audited and undertakes, where applicable, that any internal or external sub-processor will agree to be audited upon the request of a Data Controller with respect to the specific Processing activities performed on its behalf.

The said audit shall be carried out in accordance with the contractual provisions agreed between the Data Controller and the Talan Entity concerned. The audit shall be carried out by the Data Controller or by a control body composed of independent and professionally qualified members, bound by an obligation of confidentiality and selected by the Data Controller, where applicable, in agreement with the Supervisory Authority.

Audit at the request of a Supervisory Authority

A competent Supervisory Authorities may request access from the Talan Group entity to the results of the annual BCRs compliance audits and/or any BCR compliance audits requested by the Talan Group DPO and/or any audit conducted by a Data Controller.

In addition, any competent Supervisory Authority may conduct a data protection audit of any Talan Entity concerned by the application of the BCRs if required.

The Talan procedure for handling the controls of the competent Supervisory Authorities is specifically described in **Appendix 7**.

The competent Supervisory Authority is consulted to determine the necessary corrective measures to be implemented if the Processing of Personal Data is to be continued.

Audit at the specific request of the DPO

The Talan Group DPO may, following an internal or external alert, upon the request of a local DPO, or at their own discretion, request an audit of (i) BCR compliance and (ii) the rules implemented to ensure the concerned Talan Entity's protection of Personal Data. The audit results are communicated in a report to a Supervisory Authority upon its request, the local DPO, the Talan Group management and the management of the Talan Group entity concerned. They are also made available to the Data Controller.

IV. ENFORCEABILITY OF THE BCRs

1. Compliance with BCRs and implementation control by the Talan Group's network of data protection officers

To ensure compliance with the BCRs, a network of DPOs has been established within the Talan Group.

Talan undertakes to appoint, within each Talan Entity, Employees with the required skills and highest management support to monitor compliance with the BCRs ratified by Talan.

The DPOs, who are part of the GDPR governance organization, monitor Talan's legal compliance with the Applicable Law, advise on all matters relating to personal data protection, implement the overall data protection training programs, handle or advise on Personal Data Breaches and maintain an active relationship with the local Supervisory Authority.

More specifically, the Talan Group DPO is responsible for enforcing the BCRs within each Talan Entity.

Local DPOs are appointed by the Talan Group DPO. The appointees must have a good overview of the projects of the Talan Group entity concerned.

On an annual basis, the local DPOs shall report to the Talan Group DPO on all major issues related to personal data protection and more specifically on the compliance with the BCRs at a local level and monitor training programs at a local level.

Within the legal function, the Talan Group DPO as well as the regional and local DPOs are supported in their task by the local legal teams and the highest management support.

2. Third party beneficiary rights

As third party beneficiaries, Data Subjects may enforce the following provisions of the BCRs against Talan acting as a Processor:

- Duty for Talan Entities and their Employees to respect Data Controller's instructions regarding Personal Data Processing, including for Transfers of Personal Data to a third country as detailed in Article IV.3 b) below;
- Duty for Talan Entities to implement appropriate technical and organizational security measures, as indicated in Article III.3;
- Duty for Talan Entities to notify the Data Controller in case of a Personal Data Breach, as indicated in Article II.2. d);
- Duty to respect the conditions when engaging a sub-processor either within or outside the Group as indicated in Article II.2. f) and g);
- Duty for Talan Entities to cooperate with and assist the Data Controller in complying with and demonstrating compliance with the GDPR, as detailed in Article IV. 7;
- Duty for Talan to provide easy access to BCRs, as detailed in Article III.1;
- The Data Subjects' right to complain through Talan's internal complaint mechanisms as detailed in Article III.2;
- Duty for Talan Entities to cooperate with the competent Supervisory Authorities, as provided in Article IV.6;
- The Data Subjects' right to lodge a complaint before the competent Supervisory Authority and/or the competent courts, as detailed in Article IV.3 a);
- Duty for each Talan Entity exporting Personal Data outside the EEA to accept responsibility for any breach of the BCRs by sub-processors, non-EEA Talan Entities or external sub-processors established outside the EEA, who have received the Personal Data, as detailed in Article IV.3 a);
- The fact that it is the responsibility of the EEA Talan Entity, which exported the Personal Data, to demonstrate that the non-EEA Talan Entity acting as a sub-processor or any external sub-processor established outside of the EEA, Recipient of the Data, did not breach the BCRs, as set forth in Article IV.3(c);

- The right of Data Subjects to rely on the BCRs as third party beneficiaries where they cannot bring a claim against the Data Controller because the Data Controller has effectively disappeared or ceased to exist legally or has become insolvent, unless no successor entity assumes all of the Data Controller's legal obligations by contract or operation of law, in which case Data Subjects may assert their rights against such entity as provided in Article III. 2;
- Duty for Talan Entities, and their Employees, to comply with the BCRs as detailed in Article I.3 a) and b);
- Talan's obligation to create third party beneficiary rights for Data Subjects, as detailed in this same Article;
- The data protection principles listed in Article II.2;
- Duty for Talan Entities to notify the relevant Data Controller, the Talan Group DPO and the local DPO if applicable and the Supervisory Authority that the Data Controller falls under and the Supervisory Authority that the relevant Talan Entity falls under, in case of conflict between local law and the BCRs, as detailed in Article V.3;
- The obligation to list the Talan Entities, as detailed in **Appendix 1** and presented on the Talan website.

3. Liability and remedies

a) Liability towards third party beneficiaries

As set forth in Article IV.2, a Data Subject may assert certain rights under the BCRs as a third party beneficiary, if:

i) the Data Subject is not able to bring a claim against the Data Controller because the Data Controller has factually disappeared, ceased to exist in law or has become insolvent, and;

ii) the legal obligations of the Data Controller have not been transferred in their entirety, by contract or by operation of law, to another successor entity to which the Data Subject can assert their rights.

In such a case, Data Subjects shall at least be able to enforce against Talan acting as a Processor the following rights:

- Duty for Talan Entities and their Employees to respect Data Controller's instructions regarding Personal Data Processing, including for Transfers of Personal Data to a third country as detailed in Article IV.3 b) below;
- Duty for Talan Entities to implement appropriate technical and organizational security measures, as indicated in Article III.3;
- Duty to respect the conditions when engaging a sub-processor either within or outside the Group as indicated in Article II.2. f) and g);
- Duty for Talan to provide easy access to BCRs, as detailed in Article III.1;
- The Data Subjects' right to complain through Talan's internal complaint mechanisms as detailed in Article III.2;
- Duty for Talan Entities to cooperate with the competent Supervisory Authorities, as provided in Article IV.6;
- The Data Subjects' right to lodge a complaint before the competent Supervisory Authority and/or the competent courts, as detailed in Article IV.3 a);
- Duty for each Talan Entity exporting Personal Data outside the EEA to accept responsibility for any breach of the BCRs by sub-processors, non-EEA Talan Entities or external sub-processors established outside the EEA, who have received the Personal Data, as detailed in Article IV.3 a);

- The fact that it is the responsibility of the EEA Talan Entity, which exported the Personal Data, to demonstrate that the non-EEA Talan Entity acting as a sub-processor or any external sub-processor established outside of the EEA, Recipient of the Data, did not breach the BCRs, as set forth in Article IV.3(c);
- The right of Data Subjects to rely on the BCRs as third party beneficiaries where they cannot bring a claim against the Data Controller because the Data Controller has effectively disappeared or ceased to exist legally or has become insolvent, unless no successor entity assumes all of the Data Controller's legal obligations by contract or operation of law, in which case Data Subjects may assert their rights against such entity as provided in Article III. 2;
- Duty for Talan Entities, and their Employees, to comply with the BCRs as detailed in Article I.3 a) and b);
- Talan's obligation to create third party beneficiary rights for Data Subjects, as detailed in this same Article;
- The data protection principles listed in Article II.2;
- Duty for Talan Entities to notify the Talan Group DPO and the local DPO if applicable and the Supervisory Authority that the Data Controller falls under and the Supervisory Authority that the relevant Talan Entity falls under, in case of conflict between local law and the BCRs, as detailed in Article V.3;
- The obligation to list the Talan Entities, as detailed in **Appendix 1** and presented on the Talan website.

Where Article IV.2 applies, Data Subjects have judicial remedies for any breach of the third party beneficiary guaranteed rights and the right to obtain redress and where appropriate may receive compensation for any damage (both material and non-material).

Notably, Data Subjects may lodge a complaint before the competent Supervisory Authority (choice between the Supervisory Authority of the Member State of his/her habitual residence, place of work or place of alleged infringement) and before the competent court of the Member State (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. Any alternative that is more favourable to Data Subjects under national law shall apply.

Where Talan acting as a Processor and the Data Controller 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 Talan acting as a Processor.

Each Talan Entity is responsible for its own acts committed in violation of the BCRs.

However, each EEA Talan Entity exporting Personal Data outside of the EEA is responsible for violations of the committed by non-EEA Talan Entities or external sub-processors established outside of the EEA that have BCRs received Personal Data from such Talan Entity in the event that such non-EEA Talan Entities or external sub-processors established outside of the EEA are unable or unwilling to pay such compensation or comply with the BCRs.

In such a case, the relevant Exporting EEA Talan Entity undertakes to take the necessary steps to remedy the violations caused, and to pay compensation for any damages resulting from a violation of the BCRs.

The liability of the relevant Exporting EEA Talan Entity shall then be incurred to the same extent as if the breach had been committed by it in the EEA Member State in which it is domiciled, rather than by the non-EEA Talan Entity or the external sub-processor established outside the EEA.

The Exporting EEA Talan Entity concerned shall not be relieved of its liability by invoking a breach of duty by the non-EEA Talan Entity or the external sub-processor.

Each Talan Entity must have sufficient financial resources to cover compensation for the breach of the BCRs.

b) Liability towards the Data Controller

The BCRs are binding towards the Data Controller. To this end, the BCRs are integrated by a specific reference to this aspect, with the possibility of consultation by electronic means, in the Service Agreement, which complies with Article 28 of the GDPR.

The Data Controller has the right to enforce the BCRs against any Talan Entity regarding the violation it caused, and, moreover, against any relevant Exporting EEA Talan Entity in case of a violation of the BCRs or the Service Agreement by non-EEA Talan Entities or by any external sub-processor established outside the EEA.

Each Talan Entity is responsible for its own acts committed in violation of the BCRs.

However, each EEA Talan Entity exporting Personal Data outside of the EEA is responsible for violations of the BCRs committed by non-EEA Talan Entities and external sub-processors established outside of the EEA that have received Personal Data from such Talan Entity in case of such non-EEA Talan Entities or external sub-processors established outside of the EEA are unable or unwilling to pay such compensation or comply with the BCRs.

In such a case, the relevant Exporting EEA Talan Entity undertakes to take the necessary steps to remedy the violations caused, and to pay compensation for any damages resulting from a violation of the BCRs.

The liability of the relevant Exporting EEA Talan Entity shall then be incurred to the same extent as if the violation had taken place by it in the EEA Member State in which it is based instead of the non-EEA Talan Entity or the external sub-processor established outside the EEA.

The Exporting EEA Talan Entity concerned may not rely on a breach by a sub-processor (internal or external of the group) of its obligations in order to avoid its own liabilities.

Each Talan Entity must have sufficient financial resources to cover compensation for the violation of the BCRs.

c) The burden of proof

It is the responsibility of the relevant Exporting EEA Talan Entity to demonstrate that the non-EEA Talan Entity or external sub-processor established outside the EEA is not liable for any violation of the rules which has resulted in the Data Subject claiming damages.

If the Data Controller can demonstrate that it suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCRs, it will be for the Exporting EEA Talan Entity that accepted liability to prove that the BCR member outside of the EEA or the external sub-processor was not responsible for the breach of the BCRs giving rise to those damages or that no such breach took place. The relevant Exporting EEA Talan Entity may discharge itself from any liability if it can prove that the non-EEA Talan Entity or the external sub-processor established outside the EEA is not responsible for the act.

4. Accountability and other tools

As a Processor, Talan shall make available to the Data controller all information necessary to demonstrate compliance with their obligations.

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

a) Record

The Talan Entities are required to maintain in writing, including in electronic form a record of all categories of Processing activities carried out on behalf of each Data Controller, including the following:

- The name and contact details of the Talan Entity acting as a Processor, and of each Data Controller on whose behalf Talan acts, as well as the DPO;
- The categories of Processing carried out on behalf of the Data Controller;
- Where applicable, Transfers of Personal Data to countries outside the EEA including the identification of such countries;
- Where possible, a general description of the technical and organizational measures implemented.

Talan shall make the record available to the competent Supervisory Authority upon request.

b) DPIA

The Talan Entities are required to assist the Data Controller in complying with its obligation to conduct DPIAs for Processing that may pose a high risk to the rights and freedoms of Data Subjects.

In the event that such DPIAs are carried out, the Talan Entities shall provide the Data Controller with all relevant information regarding the Processing, in particular, the technical and organizational means used to implement the Processing, the location of the Personal Data, the security measures implemented (physical and technical), and if applicable, details on the sub-processor(s) etc.

However, the Talan Entities are not required to conduct DPIAs on behalf of the Data Controller. The Talan Entities only assist the Data Controllers without committing to the performance of the DPIA itself.

c) Privacy by Design and by Default

Talan undertakes to comply with the data protection principles set forth in these BCRs, regardless of the Applicable Law, unless the Applicable Law provides for stricter requirements than those set forth in these BCRs.

The Talan Entities undertake to assist the Data Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCRs in practice such as data protection by design and by default.

In this respect, when assisting the Data Controller, Talan Entities undertake, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the Processing itself, to make reasonable efforts to implement appropriate technical and organisational measures, which are designed to implement data protection principles, in an effective

manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this BCRs and protect the rights of Data Subjects.

Moreover, when assisting the Data Controller, Talan Entities undertake to implement appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility.

In addition, Talan undertakes to promote the implementation of these principles within the Group's organization through its internal policies, including training for Employees and communication actions dedicated to raising awareness of the data protection principles within the Talan Entities.

5. Sanctions

Any violation of the BCRs by a representative or Employee of a Talan Entity may result in disciplinary action or legal proceedings, in accordance with applicable labour laws, upon the decision of Talan, the Talan Group DPO, the relevant Talan Entity or the local DPO.

Therefore, the Talan Entity and the local DPO should pay particular attention to any audit results that indicate compliance issues with respect to certain representatives or Employees, including the following issues:

- Violation of the data protection principles set forth in Article II.2;
- Violation of security policies designed to implement appropriate technical and organizational measures to protect Personal Data;
- Failure to comply with obligations relating to training programs designed to educate Employees on data protection issues and principles.

6. Cooperation with Supervisory Authorities

Any Talan Entity shall cooperate with the Supervisory Authority(ies) competent for the relevant Data Controller.

Notably, Talan Entities shall take into account the advice of the competent Supervisory Authority(ies), accept to be audited by these Supervisory Authority(ies) and abide by decisions of the Supervisory Authority(ies) on any issue related to the BCRs.

Talan Entities undertake to provide the competent Supervisory Authority(ies), upon request, with any information about the processing operations covered by the BCRs.

Any dispute related to a competent Supervisory Authority's exercise of supervision of compliance with the BCRs will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State's procedural law. The Talan Entities agree to submit themselves to the jurisdiction of these courts.

7. Cooperation with the Data Controller

Any Talan Entity shall cooperate with and assist the Data Controller in complying with its obligations under the Applicable Law.

This obligation must be fulfilled within a reasonable time and to the extent reasonably possible.

V. FINAL PROVISIONS

1. Relationship between national laws and BCRs

Talan is committed to ensuring that Talan Entities and relevant Group Employees comply with the BCRs and the Applicable Law.

If the local law requires a higher level of protection for Personal Data, this takes precedence over the BCRs.

2. Onward transfers to external sub-processors

When a Talan Entity requests a non-Group entity to process Personal Data, the following safeguards must implemented:

i) Where a Talan Entity subcontracts its obligations under the Service Agreement to an external sub-processor established in the EEA or in a country recognized by the European Commission as providing an adequate protection, the external sub-processor shall be bound by a written contract stipulating that the sub-processor shall act only on the instructions of the Talan Entity concerned and shall be responsible for the implementation of adequate security and confidentiality measures as provided in Article III.3;

ii) Local DPOs shall be able to provide, in coordination with the Talan Group DPO, the EU Standard contractual clauses to the Talan Entities;

iii) Where a Talan Entity subcontracts its obligations under the Service Agreement to an external sub-processor established outside the EEA with the authorization of the Data Controller, it is required to sign a written contract with the sub-processor to ensure an adequate level of protection as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, and which ensures that the same obligations are imposed on the sub-processor as set out in the Service Agreement and under Articles IV.2,3,4,5,6 and 7 of the BCRs.

3. Actions in case of national legislation preventing respect of the BCRs

Local laws and practices affecting compliance with the BCRs

Talan Entities undertake to use these BCRs as a tool for Transfers only where they have assessed that the law and practices in the third country of destination applicable to the Processing of the Personal Data by the Talan Entity acting as data importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCRs. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the BCRs.

The Talan Entities commit that, in assessing the laws and practices of the third country which may affect the respect of the requirements contained in the BCRs, the Talan Entities have taken due account, in particular, of the following elements:

i. The specific circumstances of the Transfers or set of Transfers, and of any envisaged onward transfers within the same third country or to another third country, including:

- purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials);
- types of entities involved in the Processing (the data importer and any further recipient of any onward transfer);
- economic sector in which the Transfer or set of Transfers occur;
- categories and format of the Personal Data transferred;
- location of the Processing, including storage;
- and transmission channels used.

ii. The laws and practices of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorizing access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards.

iii. Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these BCRs, including measures applied during the transmission and to the Processing of the Personal Data in the country of destination.

Where any safeguards in addition to those envisaged under the BCRs should be put in place, the liable Talan Entity(ies), and the relevant Local DPO will be informed and involved in such assessment.

The Talan Entities shall document appropriately such assessment, as well as the supplementary measures selected and implemented. They should make such documentation available to the competent Supervisory Authorities upon request.

Any Talan Entity acting as data importer undertakes to promptly notify the data exporter if, when using these BCRs as a tool for Transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under these BCRs, including following a change in the laws in the third country or a measure (such as a disclosure request). This information should also be provided to the Data Controller and the liable Talan Entity.

Upon verification of such notification, the Talan Entity acting as data exporter, along with the liable Talan Entity(ies) and the relevant Local DPO, should commit to promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Talan Entity acting as data exporter and/or data importer, in order to enable them to fulfil their obligations under these BCRs. The same applies if a Talan Entity acting as data exporter has reasons to believe that a Talan Entity acting as its data importer can no longer fulfil its obligations under these BCRs.

Where the Talan Entity acting as data exporter, along with the liable Talan Entity(ies) and the relevant Local DPO, assesses that the BCRs – even if accompanied by supplementary measures – cannot be complied with for a Transfer or set of Transfers, or if instructed by the competent Supervisory Authority, it commits to suspend the Transfer or set of Transfers at stake, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the Transfer is ended.

Following such a suspension, the Talan Entity acting as data exporter commits to end the Transfer or set of Transfers if the BCRs cannot be complied with and compliance with the BCRs is not restored within one month of suspension. In this case, Personal Data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the Talan Entity acting as data exporter (following instructions of the Data Controller), be returned to it or destroyed in their entirety.

The liable Talan Entity(ies) and the relevant Local DPO will inform all other Talan Entities of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of Transfers is carried out by any other Talan Entity or, where effective supplementary measures could not be put in place, that the Transfers at stake are suspended or ended.

Talan Entities acting as data exporter shall monitor, on an ongoing basis, and where appropriate in collaboration with Talan Entities acting as importers, developments in the third countries to which the Talan Entities acting as data exporter have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such Transfers.

Legally binding request for disclosure of Personal Data by a law enforcement authority or state security body

The Talan Entity acting as data importer will promptly notify the data exporter if it:

a) receives a legally binding request by a public authority under the laws of the country of destination, or of an another third country, for disclosure of Personal Data transferred pursuant to the BCRs; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;
b) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCRs in accordance with the laws of the country of destination; such notification will include all information available to the Talan Entity acting as data importer.

This information should also be provided to the Data Controller and the liable Talan Entity.

If prohibited from notifying the data exporter, and/or the Data Controller and/or the Data Subject, the Talan Entity acting as data importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the data exporter / Data Controller.

The Talan Entity acting as data importer will provide the data exporter / Data Controller, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Talan Entity acting as data importer is or becomes partially or completely prohibited from providing the data exporter / Data Controller with the aforementioned information, it will, without undue delay, inform the data exporter / Data Controller accordingly.

The Talan Entity acting as data importer will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCRs, and shall make it available to the competent Supervisory Authority(ies) upon request.

The Talan Entity acting as data importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to

consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.

The Talan Entity acting as data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the Talan Entity acting as data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

The Talan Entity acting as data importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter / Data Controller. It will also make it available to the Supervisory Authority(ies) upon request.

The Talan Entity acting as data importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

This procedure for handling request for disclosure of Personal Data by a law enforcement authority or state security body is described in **Appendix 7**.

In any case, transfers of Personal Data by a Talan 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.

4. Amendments to the BCRs

In the event of changes to the Applicable Law or Talan's procedures, the provisions of these BCRs may be amended at Talan's discretion, in coordination with the Talan Group DPO.

The Talan Group DPO will keep track of and record any amendment, substantial or not, to the BCRs and provide the necessary information systematically to the Clients and to Supervisory Authorities upon request.

The Talan Group DPO also maintains up-to-date a comprehensive list of Talan Entities and of the sub-processors involved in Processing activities made accessible to the Clients, Data subjects and Supervisory Authorities.

Talan undertakes to provide the Talan Entities, Clients, and Data Subjects with appropriate information regarding any amendments to the BCRs, including to the list of Talan Entities, without undue delay.

Any change to the BCRs that may possibly significantly affect the BCRs or be detrimental to the level of protection they provide e.g. changes to the binding character, change to the list of Talan Entities will be communicated in advance to the relevant Supervisory Authorities via the BCR Lead with a brief explanation of the reasons for the update.

In such a case, Talan also undertakes to inform the Data Controller in such a timely fashion that the Data Controller has the possibility to object to the change or to terminate the Service Agreement before the modification is made.

Once a year, Talan undertakes to notify the relevant Supervisory Authorities via the BCR Lead of any changes to the BCRs or to the list of Talan Entities, with the brief explanation of the reasons for the changes.

No Transfer will be made to a new Talan entity until that new entity is effectively bound by the BCRs and can ensure compliance.

5. Termination

Any Talan Entity acting as data importer, which ceases to be bound by the BCRs shall, at the choice of the Data Controller, delete or return all the Personal Data transferred to the Data Controller and delete the copies thereof and certify to the Data Controller that it has done so, unless legislation imposed upon them requires storage of the Personal Data transferred. In that case, the relevant Talan Entity shall inform the Data Controller and warrant that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

6. Non-compliance

Talan Entities should promptly inform the data exporter / Data Controller if it is unable to comply with the BCRs, for whatever reason, including the situations further described in Article V. 3. of the BCRs.

Where a Talan Entity is in breach of the BCRs or unable to comply with them, the data exporter should suspend the Transfer.

The Talan Entity should, at the choice of the Data Controller (and failing that, at the choice of the data exporter), immediately return or delete the Personal Data that has been transferred under the BCRs in its entirety, where:

- the Data Controller and/or data exporter has suspended the Transfer, and compliance with this BCRs is not restored within a reasonable time, and in any event within one month of suspension; or
- the Talan Entity is in substantial or persistent breach of the BCRs; or
- the Talan Entity fails to comply with a binding decision of a competent court or competent Supervisory Authority regarding its obligations under the BCRs.

The same commitments apply to any copies of the data. The Talan Entity should certify the deletion of the data to the data exporter / Data Controller.

Until the data is deleted or returned, the Talan Entity should continue to ensure compliance with the BCRs.

In case of local laws applicable to the Talan Entity that prohibit the return or deletion of the transferred Personal Data, the Talan Entity should warrant that it will continue to ensure compliance with the BCRs, and will only process the data to the extent and for as long as required under that local law.

VI. Appendixes

1. List of Talan Entities bound by the BCRs
2. General description of the BCRs' material scope
3. Template Data Protection clauses to be included in Service Agreements with Clients
4. Procedure for handling Data Subject requests
5. Talan Group BCRs Compliance and Audit Policy
6. GDPR Governance Policy
7. Competent Authority Control Management Policies

APPENDIX 1 – LIST OF TALAN ENTITIES BOUND BY THE BCRs

GEOGRAPHICAL ZONE	NB	COUNTRY	NB	NAME OF THE ENTITY	DESCRIPTION OF ACTIVITY	CONTACT DETAILS
EUROPEAN UNION	9	France	6	Talan Corporate	Talan Corporate is the principal entity of Talan Group, it constitutes the decision-making entity and provides the support services to all entities of the Group (strategy, finance, legal, marketing, human resources, IT; etc.). As such, TALAN CORPORATE has delegated data protection responsibilities. The group's legal and compliance officer for data protection is attached to this entity.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 515 132 694 R.C.S. PARIS
				Talan Holding	Talan Holding is the holding company for Talan Group. Talan Holding has no commercial activity, holds shares and manages its subsidiaries.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 887 633 733 R.C.S. PARIS

				Talan SAS	TALAN SAS operates in France and abroad in the following fields: IT services, engineering, consulting and technical assistance in information systems.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 488 601 337 R.C.S. PARIS
				Talan Consulting	Management consulting and information systems.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 481 088 789 R.C.S. PARIS
				Talan LABS	Provision of services in the IT field, creation and publishing of software, marketing (sale) of hardware and software.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 887 633 733 R.C.S. PARIS
				Talan Solutions	Services and expertise, development consulting, research and engineering. The study, design, implementation, development of IT projects, then associated training projects. Stake acquisition in all companies and portfolio management thus constituted.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 508 878 386 R.C.S. PARIS

		Spain	1	Talan Consulting Espana	IT services and technical assistance	Limited liability company registered in the Madrid Trade and Companies Register under the identification number 97960423 Paseo de la Castellana 200 Madrid 28046, SPAIN
		Belgium	1	TALAN Belgium	IT services and technical assistance	Limited liability company registered in the Brussels Trade and Companies Register under the identification number 778 693 036 Avenue Arnaud Fraiteur 15 1050 Ixelles, BELGIUM
		Luxembourg	1	Talan Luxembourg	IT services and technical assistance	Limited liability company registered with the Luxembourg Trade and Companies Register under identification number 101418 21 rue Glesener 1631 Luxembourg, LUXEMBOURG
EUROPE	3	United Kingdom	2	Business Data Partners Ltd	IT services and technical assistance	Private limited Company registered under the laws of England and Wales with the Companies House under the identification number 09277132 28 Lime Street, London, EC3M 7HR - 2nd floor, UNITED KINGDOM

				Talan Consulting UK Ltd	IT services and technical assistance	Private Limited Company registered under the laws of England and Wales with the Companies House under identification number 05388143 28 Lime Street, London, EC3M 7HR - 2nd floor, UNITED KINGDOM
		Switzerland	1	Talan Suisse	IT services and technical assistance	Limited liability company registered with the Geneva Trade and Companies Register under the identification number 106.832.761 Place Ruth-BÖSIGER 6, 1201 Genève, SWITZERLAND
NORTH AMERICA	3	Canada	2	Talan Canada Inc	IT services and technical assistance	Canadian Société par actions registered under the laws of Canada with the Trade and Companies Register of Quebec under the identification number 1163837454 700-60 rue Saint-Jacques Montréal, Québec, H2Y1L5, CANADA
				Talan Conseil Canada INC	IIT services and technical assistance	Canadian Société par actions registered under the laws of Canada with the Trade and Companies Register of Quebec under the identification number 1169006146

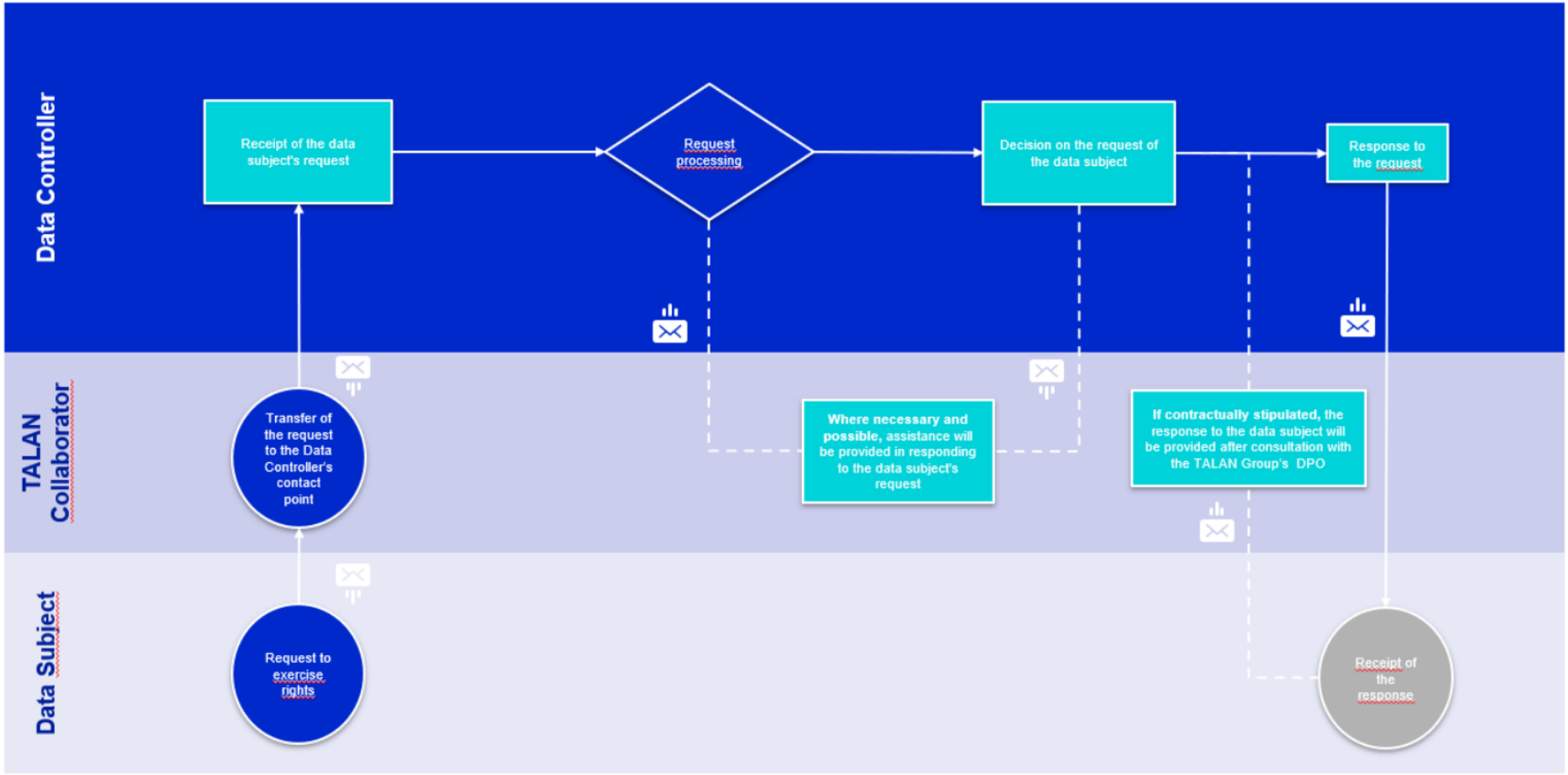
						700-60 rue Saint Jacques Montreal, Quebec, H2Y1L5, CANADA
		USA	1	Talan LLC	IT services and technical assistance	Limited liability company registered under the laws of the State of Delaware with the Delaware Trade and Companies Register under the identification number 20-4193242 33 Irving Place - New York, 10003 New York, USA
AFRICA	1	Tunisia	1	Talan Tunisie Consulting	Nearshore center who works exclusively for the Talan Group's companies and their clients: Software development, IT projects, Third Party Application Maintenance (TPMA).	Limited liability company registered with the Tunis Trade and Companies Register under the identification number 1325392 10 rue de l'Energie Solaire, Impasse N°1 2035 Tunis, TUNISIA
TOTAL	16		16			

APPENDIX 2: GENERAL DESCRIPTION OF THE BCRs' MATERIAL SCOPE

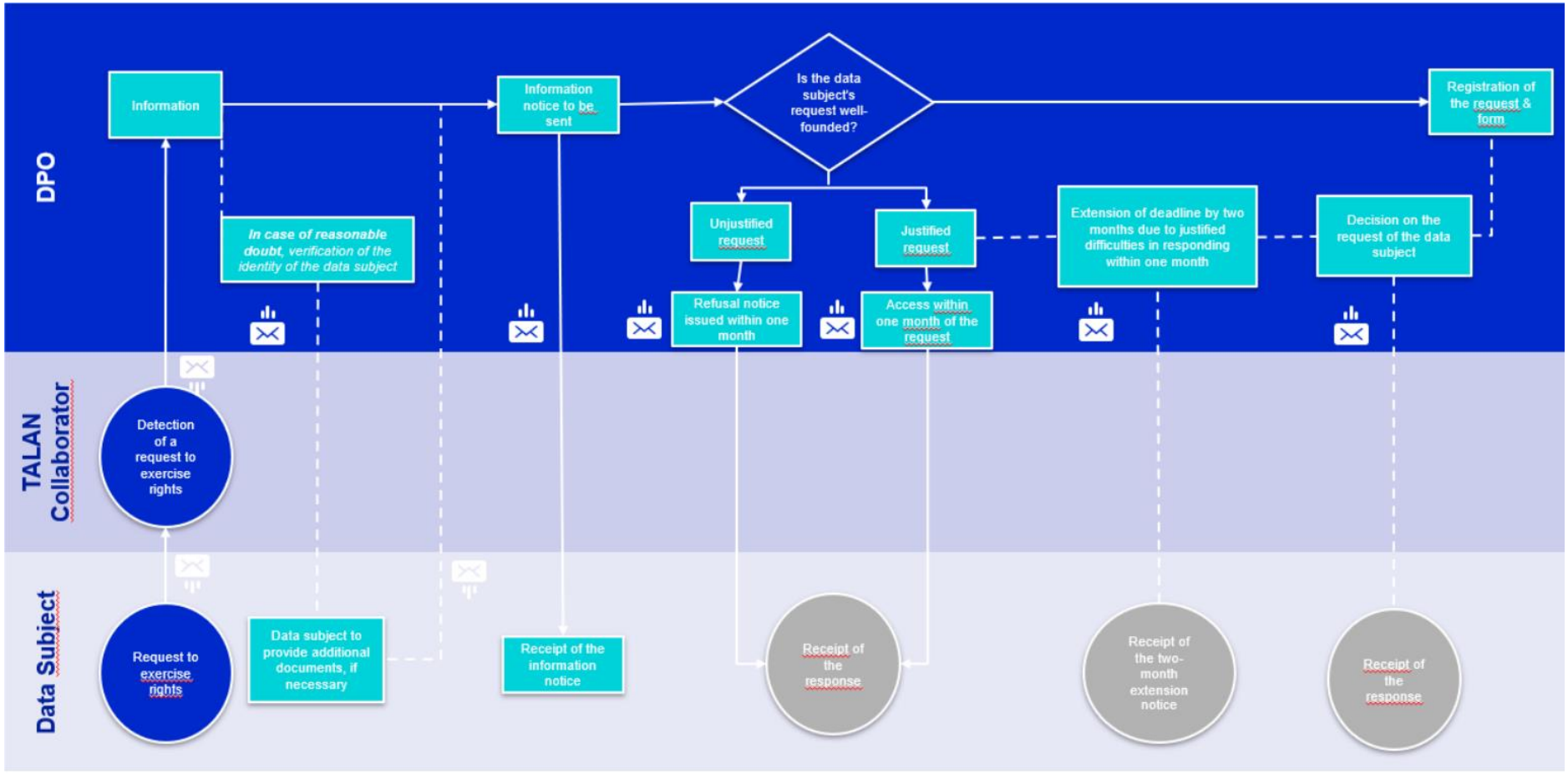
Purposes of data transfer and further processing	TALAN processes the personal data of its Clients in order to carry out their projects related to IT services, management consulting, software creation and publishing, technical assistance, etc. The purpose of transferring the Client's personal data is to enable the most efficient entity of the TALAN Group, depending on the Client and the nature of the services, to provide the services agreed with the Client.
Nature of the data transfer	*TALAN LLC (US)* Provision of IT services and technical assistance. *TALAN TUNISIE CONSULTING (Tunisia)* Provision of Software development services, IT services and technical assistance, Third Party Application Maintenance (TPAM).
Categories of personal data transferred	The categories of personal data processed by TALAN Group, in accordance with applicable law, depend on the services provided to the Client and may include, but are not limited to: - identification data or personal details (e.g. names, address, telephone number, e-mail address…) - data on working life (e.g. position, company of affiliation, employment contract, recruitment date, employee identification number, professional contact details…) - economic and financial data (e.g. tax, banking details…) - location data (e.g. access information) - connection and usage data (e.g. logs, IP addresses…).
Types of special categories of personal data transferred (if any)	TALAN may process sensitive data such as information about health, including any medical condition, health and sickness records. Where sensitive personal data is processed by the TALAN Group, in accordance with applicable law, additional measures apply.
Categories of data subjects whose personal data are transferred	The categories of data subjects depend on the services provided to Client, and may include, but are not limited to: (i) prospects, customers, business partners and vendors of Clients (who are natural persons); (ii) employees or contact persons of Client's prospects, customers, business partners and vendors; (iii) employees, agents, consultants, freelancers of Clients (who are natural persons); and (iv) users of Client authorized by Client to use the services.

APPENDIX 2: GENERAL DESCRIPTION OF THE BCRs' MATERIAL SCOPE

1. Procedure for handling a Data Subject's complaint or request where the Talan Group acts as a Processor


Data Controller
Receipt of the data subject's request
Request processing
Decision on the request of the data subject
Response to the request
TALAN Collaborator
Transfer of the request to the Data Controller's contact point
Where necessary and possible, assistance will be provided in responding to the data subject's request
If contractually stipulated, the response to the data subject will be provided after consultation with the TALAN Group's DPO
Data Subject
Request to exercise rights
Receipt of the response

2. Procedure for handling a Data Subject's complaint or request where the Talan Group acts as a Processor and the Data Controller has disappeared



Competent Authority Control Management Policy

Date	Version	Author	Modification
13/01/2023	0.1	DPO	Creation
14/02/2024	0.2	DPO	Amended to include CNIL feedback in the context of the BCR-P approval procedure

Contents

Issues and purposes

The purpose of this policy is to provide for the management of requests from competent supervisory authorities regarding personal data protection. The purpose of this policy is to ensure that the conditions under which requests for control from competent authorities that may conduct investigations and audits of the Talan Group comply with the *Binding Corporate Rules* (BCRs) adopted by the relevant entities of the Group.

The main challenge of this policy is therefore to ensure the Talan Group's compliance with the current standards and regulations on personal data protection, minimizing the risk of infringements and maintaining a good relationship with the competent authorities, providing a clear and transparent framework for communication and cooperation during their controls.

- # Interactions with the competent supervisory authorities for the protection of personal data

1. 2.1. Procedure for handling the controls of the competent supervisory authorities

2.1.1. Preparation for the controls

The Talan Group DPO ensures that key Talan Group personnel, who can be consulted by the relevant authorities, have a clear understanding of their responsibility for the protection of personal data and the obligations arising from the Talan Group BCRs. The Talan Group DPO ensures that there is up-to-date documentation of all procedures, policies and processing activities relating to personal data within the Talan Group.

2.1.2. Receipt of control requests

When a Talan Group employee receives a request for information or control from a competent authority in matters of personal data protection, he/she informs the Talan Group DPO, or the local DPO, identified within the Talan Group entity concerned, who is responsible for informing the Group DPO.

2.1.3. Response to requests

After assessing and analyzing the request of the competent supervisory authority, the Talan Group's DPO, or the local DPO if the Talan Group's DPO delegates the management of the request to the latter, responds to the request of the competent supervisory authority within the timeframe indicated by the latter, or in the absence of a timeframe within a reasonable timeframe that may not exceed one (1) month as of the receipt of the request.

The Talan Group DPO, or the local DPO responsible for the request, is the only person authorized to judge the response to be sent to the requesting authority as well as the appropriate documentation to be provided.

2.1.4. Implementation of corrective measures and analysis of the reasons for the control

If, as a result of the response, the competent authority issues an opinion or initiates an advanced control procedure, the person in charge of management makes every effort to comply with the competent supervisory authority's requests. The competent supervisory authority is consulted to determine the necessary corrective measures to be implemented if the processing of personal data is to be continued. In this case, the Talan Group implements all the necessary corrective measures to remedy the issues identified during the control and to ensure compliance and respect of the personal data protection regulations.

Once the audit is completed, the Talan Group's DPO, or the local DPO conducts an analysis of the reasons and factors that led to the audit and how the processing and management of personal data can be improved within the Talan Group or the Talan Group entity concerned.

2.1.5. Follow-up of the controls

The Talan Group DPO maintains detailed documentation of all interactions with the relevant authorities, including responses provided and actions taken in response to the findings of the relevant authorities.

2. 2.2. Mandatory notifications to the competent supervisory authorities

Where required by the Talan Group BCRs, the GDPR or any applicable laws or regulations, the relevant Talan Group entities undertake to obtain the necessary authorizations or notify the necessary information to the relevant supervisory authorities.

In particular, in accordance with the commitments formalized in the Talan Group's BCRs, each concerned entity of the Talan Group undertakes, when it has reason to believe that current or future legislation applicable to it may prevent it from complying with the instructions received from a Data Controller or from fulfilling its obligations under the BCRs or the service agreement, to inform the persons listed below without delay.

- Talan Group DPO and local DPO (if not already informed);
- The relevant Data Controller, who may suspend the transfer of data and/or terminate the agreement;
- The supervisory authority to which the Data Controller is subject;
- The supervisory authority of the Talan Group entity concerned.

- **Request from a law enforcement authority or state security agency**

The Talan Group entity concerned acting as data importer will promptly notify the data exporter if it:

c) receives a legally binding request by a public authority under the laws of the country of destination, or of an another third country, for disclosure of personal data transferred pursuant to the BCRs; such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided;

d) becomes aware of any direct access by public authorities to personal data transferred pursuant to the BCRs in accordance with the laws of the country of destination; such notification will include all information available to the Talan Group entity concerned acting as data importer.

This information should also be provided to the Data Controller and the liable Talan Group entity.

If prohibited from notifying the data exporter, and/or the Data Controller and/or the Data Subject, the Talan Group entity concerned acting as data importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the data exporter / Data Controller.

The Talan Group entity concerned acting as data importer will provide the data exporter / Data Controller, at regular intervals, with as much relevant information as possible on the requests received

(in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Talan Group entity concerned acting as data importer is or becomes partially or completely prohibited from providing the data exporter / Data Controller with the aforementioned information, it will, without undue delay, inform the data exporter / Data Controller accordingly.

The Talan Group entity concerned acting as data importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by the BCRs, and shall make it available to the competent supervisory authority(ies) upon request.

The Talan Group entity concerned acting as data importer will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity.

The Talan Group entity concerned acting as data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the Talan Group entity concerned acting as data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules.

The Talan Group entity concerned acting as data importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter / Data Controller. It will also make it available to the supervisory authority(ies) upon request.

The Talan Group entity concerned acting as data importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, transfers of personal data by a Talan Group 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.

REGLES D'ENTREPRISE CONTRAIGNANTES APPLICABLES AUX SOUS-TRAITANTS

(BINDING CORPORATE RULES - PROCESSOR, OU BCR-P)

TALAN en qualité de Sous-traitant

VII. INTRODUCTION

8. Objet

Afin de garantir le plus haut niveau de protection aux données que Talan traite, Talan a adopté des Règles d'entreprise contraignantes. Ces Règles d'entreprise contraignantes visent à établir des principes et des processus de protection des données que chaque Entité Talan s'engage à appliquer afin de garantir un niveau élevé de protection des Données à caractère personnel au sein de Talan.

9. Champ d'application des BCR

d) Champ d'application géographique

Les présentes BCR couvrent toutes les Données à caractère personnel transférées et traitées entre les Entités Talan dans le cadre des activités de Talan agissant en qualité de Sous-traitant, quelle que soit l'origine de ces Données à caractère personnel.

En pratique, cela signifie que les BCR s'appliqueront aux Données à caractère personnel transférées depuis :

- Une Entité Talan de l'EEE à une autre Entité Talan de l'EEE ;
- Une Entité Talan de l'EEE à une Entité Talan non EEE ;
- Une Entité Talan non EEE à une Entité Talan de l'EEE ;
- Une Entité Talan non EEE à une autre Entité Talan non EEE.

Les Entités Talan sont listées en **Annexe 1** des BCR.

e) Champ d'application matériel

Les BCR s'appliquent aux Traitements de Données à caractère personnel par le Groupe Talan agissant en tant que Sous-traitant, suivant les instructions de ses Clients, Responsables de traitement, quelle que soit la nature ou la catégorie de la Personne concernée ou des Données à caractère personnel. Une description générale du champ d'application matériel des BCR est fournie à l'**Annexe 2** des présentes BCR.

10. Caractère contraignant des BCR

Chaque Entité Talan, y compris ses Employés, est tenue de respecter les Règles d'entreprise contraignantes.

f) A l'égard des Entités Talan

En pratique, l'Accord intra-groupe a été conclu entre TALAN CORPORATE et chaque Entité Talan listée en **Annexe 1** des présentes BCR.

En signant l'Accord intra-groupe, chaque Entité Talan a accepté d'être entièrement liée par les dispositions des BCR s'engageant ainsi à les respecter et à les mettre en œuvre au sein de sa propre organisation.

g) A l'égard des Employés

Les BCR font partie des politiques internes du Groupe via le Code de Conduite de Talan qui prévoit que les Employés de chacune des Entités Talan sont soumis aux dispositions des BCR.

A cet égard, lorsque cela est nécessaire, ou à tout moment, les Employés de chacune des Entités Talan peuvent se rapprocher du DPO du Groupe Talan (dpo@talan.com) pour obtenir de l'aide ou des informations sur le respect des règles en matière de protection des Données à caractère personnel.

Le Code de Conduite de Talan rappelle aux Employés de chacune des Entités Talan que tout manquement aux règles et mesures de sécurité concernant le respect de la Loi applicable ou des règles du Groupe Talan, notamment les BCR, est susceptible d'engager la responsabilité du collaborateur et d'entraîner à son encontre des avertissements, voire des sanctions disciplinaires proportionnées à la gravité des faits concernés. Dans ce dernier cas, les procédures prévues par le règlement intérieur et les législations locales seront appliquées.

Le Code de Conduite de Talan prévoit également que Talan se réserve le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de violation de la Loi applicable.

Par ailleurs, comme détaillé à l'Article III.4 des présentes BCR, les Employés de chacune des Entités Talan sont informés des dispositions des BCR et des obligations qui en découlent par le biais de communications internes et de programmes de formation couvrant la mise en œuvre des BCR.

h) A l'égard des Clients de Talan

Lorsque Talan agit en tant que Sous-traitant, il s'engage à conclure des Contrats de service conformes aux exigences de l'article 28 du GDPR.

En outre, Talan s'engage à se conformer aux BCR qui seront rendues contraignantes pour les Entités Talan à l'égard d'un Responsable de traitement par le biais d'une référence spécifique dans le Contrat de service.

En tout état de cause, un Responsable de traitement pourra faire valoir les BCR à l'encontre de toute Entité Talan pour les violations des BCR qu'elle aurait causées, conformément aux dispositions énoncées à l'Article IV.3.b).

VIII. DEFINITIONS ET PRINCIPES RELATIFS A LA PROTECTION DES DONNEES

11. Définitions

Les termes et expressions utilisés dans les BCR sont définis comme suit et sont interprétés, en toutes circonstances, conformément au Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

« Accord intra-groupe » désigne l'accord juridiquement contraignant ayant pour objet de rendre les BCR contraignantes pour les Entités Talan.

« Analyse d'impact sur la protection des données » ou **« AIPD »** désigne un processus visant à décrire un Traitement, à évaluer sa nécessité et sa proportionnalité et à aider à gérer les risques pour les droits

et libertés des personnes physiques résultant de ce Traitement en les évaluant et en déterminant les mesures pour y remédier.

« Autorité(s) de contrôle » ou **« Autorité(s) de protection des données »** désigne les autorités publiques indépendantes de l'Union européenne chargées de contrôler l'application du RGPD afin de protéger les droits fondamentaux et les libertés des personnes physiques en ce qui concerne les Traitements de Données à caractère personnel et de faciliter la libre circulation des Données à caractère personnel au sein de l'UE. **« Clauses types de l'UE »** désigne les clauses contractuelles émises par la Commission européenne pour encadrer les Transferts de données selon la Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021.

« Données sensibles » désigne les Données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

« Client(s) » ou « Responsable (s) de traitement » désigne toute personne physique ou morale à laquelle Talan fournit des services, en vertu d'un Contrat de service et qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement de Données à caractère personnel.

« Contrat de service » désigne un accord écrit conclu entre un Responsable de traitement et un Sous-traitant, en vertu duquel le Sous-traitant fournit des services au Responsable de traitement et qui implique le Traitement de Données à caractère personnel par le Sous-traitant selon les instructions du Responsable de traitement.

« Délégué à la protection des données » ou **« DPO »** désigne les Employés désignés possédant une connaissance experte de la législation et des pratiques en matière de protection des données, dédiés à conseiller, informer et contrôler le respect de la Loi applicable, et qui font partie du réseau de délégués à la protection des données décrit à l'Article IV. 1.

« DPO local » désigne un Employé travaillant pour une Entité Talan dont la fonction est de contrôler que les Employés connaissent et respectent la Loi applicable et les politiques, procédures et lignes directrices de Talan en la matière, et plus particulièrement les BCR.

« DPO du Groupe Talan » désigne la personne chargée, au niveau du Groupe Talan, de veiller à la connaissance et au respect par les Entités Talan et leurs Employés de la Loi applicable et des politiques, procédures et lignes directrices de Talan en matière de protection des Données à caractère personnel, et plus particulièrement des BCR**.**

« Destinataire(s) » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de Données à caractère personnel, qu'il s'agisse ou non d'un tiers ; les autorités qui sont susceptibles de recevoir communication de Données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'UE ou au droit d'un État membre ne sont toutefois pas considérées comme des Destinataires.

« Données à caractère personnel » désigne toute information relative à une personne physique identifiée ou identifiable (c'est-à-dire la « **Personne concernée** »). Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou par un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

« Employé » désigne tout membre actuel, ancien ou futur du personnel de Talan, y compris les travailleurs intérimaires et les stagiaires.

« Entité(s) Talan » désigne toute entité du Groupe ayant ratifié l'Accord intra-groupe et par conséquent, étant liée par les BCR.

« Entité(s) Talan de l'EEE » désigne toute Entité Talan située dans l'Espace économique européen (ou **« EEE »**).

« Entité(s) Talan non EEE » désigne toute Entité Talan située en dehors de l'EEE.

« Entité Talan de l'EEE exportatrice » désigne l'Entité Talan, située au sein de l'EEE, qui transfère les Données à caractère personnel en dehors de l'EEE.

« Loi applicable » désigne toute réglementation applicable en matière de protection des Données à caractère personnel qui pourrait s'appliquer et notamment (i) le RGPD et (ii) toute loi et réglementation nationale applicable au traitement des Données à caractère personnel, étant précisé que le RGPD prévaut sur les lois et règlements nationaux, sauf si ces derniers sont plus contraignants.

« Personne(s) concernée(s) » désigne toute personne physique identifiée ou identifiable dont les Données à caractère personnel sont traitées. Les personnes concernées sont des tiers bénéficiaires en ce qui concerne le Transfert de leurs Données à caractère personnel.

« Règles d'entreprise contraignantes » ou **« BCR »** ou **« BCR-P »** désigne une politique de protection des données à laquelle adhère un Sous-traitant pour les Transferts ou un ensemble de Transferts de Données à caractère personnel vers un sous-traitant ultérieur dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique commune. Pour le Groupe Talan, elles constituent le présent document ainsi que ses annexes.

« Règlement général sur la protection des données » ou **« RGPD »** désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation de ces données.

« Sous-traitant » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des Données à caractère personnel pour le compte du Responsable de traitement.

« Talan », **« Groupe »** ou **« Groupe Talan »** désigne toutes les entités détenues et/ou contrôlées directement ou indirectement par TALAN CORPORATE.

« Traitement(s) » désigne toute opération ou ensemble d'opérations effectuées sur des Données à caractère personnel ou sur des ensembles de Données à caractère personnel, par des moyens automatisés ou non, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison, la restriction, l'effacement ou la destruction.

« **Transfert(s) »** désigne la divulgation, la transmission ou le processus de mise à disposition des Données à caractère personnel à tout tiers.

« **Violation(s) de Données à caractère personnel »** désigne la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des Données à caractère personnel transmises, stockées ou traitées d'une autre manière, qu'elles résultent d'une violation de la sécurité ou non.

« **L'Autorité chef de file** » désigne l'Autorité de contrôle compétente dans le cadre de la procédure d'approbation des présentes BCR (c'est-à-dire l'Autorité de contrôle française, la « CNIL »).

12. Principes relatifs à la protection des données de Talan

Chaque Entité Talan s'engage à respecter les principes relatifs à la protection des données énoncés dans les présentes BCR comme suit, indépendamment de la Loi applicable en matière de protection des données, à moins que la Loi applicable en matière de protection des données ne prévoit des exigences plus strictes que celles énoncées dans les BCR. Tous ces principes sont promus et mis en œuvre au sein de chaque Entité Talan par le biais d'un ensemble de politiques et de formations sur la protection des Données à caractère personnel.

i) Transparence, loyauté et licéité

Chaque Entité Talan s'engage à être transparente en ce qui concerne ses activités de Traitement et a le devoir général d'aider le Responsable de traitement à se conformer à la Loi applicable.

Les Entité Talan fourniront au Responsable de traitement une coopération et une assistance raisonnables dans un délai raisonnable pour l'aider à s'acquitter de ses obligations respectives en vertu de la Loi applicable, dans la mesure où le Responsable de traitement, dans le cadre de son utilisation des services, n'a pas la capacité raisonnable de s'acquitter de ces obligations. Il peut s'agir, par exemple, de la responsabilité de se conformer à certaines instructions stipulées dans le contrat ou tout autre document juridiquement contraignant conclu avec le Responsable de traitement, notamment d'aider le Responsable de traitement à se conformer à l'obligation d'informer et d'expliquer aux Personnes concernées la manière dont leurs Données à caractère personnel seront traitées au moment de la collecte de ces données.

j) Limitation de la finalité

Chaque Entité Talan a l'obligation de traiter les Données à caractère personnel uniquement pour le compte du Responsable de traitement et conformément à ses instructions documentées, y compris en ce qui concerne les Transferts de Données à caractère personnel vers un pays tiers, à moins qu'elle ne soit tenue d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel elle est soumise. Dans ce cas, l'Entité Talan concernée informe le Responsable de traitement de cette obligation légale avant le Traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public (article 28, paragraphe 3, du RGPD). Dans d'autres cas, si une Entité Talan ne peut respecter ces dispositions pour une raison quelconque, elle accepte d'informer promptement le Responsable de traitement de son incapacité à s'y conformer, auquel cas le Responsable de traitement est autorisé à suspendre le Transfert de Données et/ou à résilier le Contrat de service. À la résiliation de la prestation de services en lien avec le Traitement, l'Entité Talan concernée supprime ou renvoie, au choix du Responsable de traitement, toutes les Données à caractère personnel transférées au Responsable de traitement et en supprime les copies, et certifie à ce dernier avoir exécuté cette tâche, à moins que la Loi applicable n'exige la conservation des Données à caractère personnel transférées. Dans ce cas, l'Entité Talan concernée informe le Responsable de traitement de la situation et lui garantit d'assurer la confidentialité des Données à caractère personnel transférées et à ne plus les traiter activement.

k) Qualité des Données à caractère personnel

Chaque Entité Talan a l'obligation générale d'aider le Responsable de traitement à respecter la Loi applicable, en particulier :

- Chaque Entité Talan exécute les mesures nécessaires lorsque le Responsable de traitement en fait la demande, en vue de la mise à jour, de la correction ou de la suppression de Données à caractère personnel. Chaque Entité Talan notifie les rectifications ou suppressions de Données à caractère personnel à chaque Entité Talan à laquelle les données avaient été communiquées ;

- Chaque Entité Talan exécute les mesures nécessaires lorsque le Responsable de traitement en fait la demande, en vue de la suppression ou de l'anonymisation des Données à caractère personnel à compter du moment où le formulaire d'identification n'est plus nécessaire. Chaque Entité Talan notifie les suppressions ou anonymisations de Données à caractère personnel à chaque entité à laquelle les Données à caractère personnel avaient été communiquées.

l) Sécurité

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, chaque Entité Talan doit mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque que présente le Traitement, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des Données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
c) des moyens permettant de rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement.

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le Traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Le Responsable de traitement et les Entités Talan doivent prendre des mesures pour s'assurer que toute personne physique agissant sous l'autorité du Responsable de traitement ou des Entités Talan et ayant accès aux Données à caractère personnel, ne les traite que sur instruction du Responsable de traitement, à moins qu'elle ne soit tenue de le faire en vertu de la Loi applicable.

Chaque Entité Talan doit également aider le Responsable de traitement à garantir le respect des obligations de notifier l'Autorité de contrôle compétente et les Personnes concernées, le cas échéant, en cas de violation de Données à caractère personnel, réaliser une AIPD et consulter l'Autorité de contrôle compétente avant le Traitement, si nécessaire telles que prévues aux articles 32 à 36 du RGPD compte tenu de la nature du Traitement et des informations à la disposition de chaque Entité Talan (article 28, paragraphe 3, point f), du RGPD).

Chaque Entité Talan doit mettre en œuvre des mesures techniques et organisationnelles appropriées qui répondent, au minimum, aux exigences de la Loi applicable au Responsable de traitement ainsi que toute mesure particulière existante énoncée dans le Contrat de service. Les Entités Talan notifient au Responsable de traitement toute Violation de Données à caractère personnel dans les

meilleurs délais après en avoir pris connaissance. En outre, toute Entité Talan agissant en tant que sous-traitant ultérieur est tenue de notifier à l'Entité Talan agissant en tant que sous-traitant principal et au Responsable de traitement, toute Violation de Données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

m) Droits des Personnes concernées

Chaque Entité Talan mettra en œuvre des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, lorsque le Responsable de traitement lui en fait la demande, afin de l'aider à s'acquitter de son obligation de donner suite aux demandes que les Personnes concernées lui adressent en vue d'exercer leurs droits prévus au chapitre III du RGPD (article 28, paragraphe 3, point e), du RGPD) tels que le droit d'être informé, le droit d'accès aux Données à caractère personnel, les droits de rectification et de suppression, le droit à la portabilité, le droit d'opposition et le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé. Les Entités Talan doivent communiquer toute information utile pour aider le Responsable de traitement à s'acquitter de son obligation de respecter les droits des Personnes concernées. Chaque Entité Talan transmettra au Responsable de traitement les demandes des Personnes concernées sans y répondre, à moins qu'elle ne soit autorisée à le faire.

L'**Annexe 4** et l'article III. 2 de ces BCR décrivent la procédure de gestion des demandes de droits des personnes concernées que doivent suivre les Entités Talan.

n) Sous-traitance au sein du Groupe Talan

Les Données à caractère personnel ne peuvent être sous-traitées par d'autres Entités Talan que si celles-ci disposent de l'autorisation écrite préalable, spécifique ou générale, du Responsable de traitement. Le Contrat de service précisera si une autorisation préalable générale accordée au début du service suffit ou si une autorisation spécifique sera requise pour chaque nouveau sous-traitant ultérieur. Si une autorisation générale est accordée, le Responsable de traitement doit être informé par l'Entité Talan agissant en tant que sous-traitant principal de toute modification prévue concernant l'ajout ou le remplacement d'une Entité Talan agissant en tant que sous-traitant ultérieur, et ce suffisamment en amont pour que le Responsable de traitement ait la possibilité de s'opposer à la modification ou de résilier le Contrat de service avant que les Données à caractère personnel ne soient communiquées à la nouvelle Entité Talan agissant en tant que sous-traitant ultérieur.

o) Transferts ultérieurs vers des sous-traitants ultérieurs externes

Les Données à caractère personnel ne peuvent être sous-traitées par des entités non-membres des BCR que si celles-ci disposent de l'autorisation écrite préalable, spécifique ou générale, du Responsable de traitement. Si une autorisation générale est accordée, le Responsable de traitement doit être informé par l'Entité Talan concernée de toute modification prévue concernant l'ajout ou le remplacement de sous-traitants ultérieurs, et ce suffisamment en amont pour que le Responsable de traitement ait la possibilité de s'opposer à la modification ou de résilier le Contrat de service avant que les Données à caractère personnel ne soient communiquées aux nouveaux sous-traitants ultérieurs.

Lorsque l'Entité Talan sous-traite ses obligations au titre du Contrat de service, avec l'autorisation du Responsable de traitement, celle-ci a impérativement recours à un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit de l'État membre conclu avec le sous-traitant ultérieur, prévoyant une protection adéquate telle qu'énoncée aux articles 28, 29, 32, 45, 46 et 47 du RGPD et garantissant que les mêmes obligations de protection des données établies dans le Contrat de

service entre le Responsable de traitement et l'Entité Talan concernée, ainsi qu'aux Articles I.3, II.2, IV.2, IV.4. a), IV.6, IV.7, V.1, V.2, V.3 des présentes BCR, soient imposées au sous-traitant ultérieur, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences du RGPD (article 28, paragraphe 4, du RGPD).

IX. EFFICACITE DES BCR

13. Accès des Personnes concernées aux BCR

Les Personnes concernées ont le droit d'accéder facilement aux BCR.

Par conséquent, Talan s'engage à ce que les Personnes concernées bénéficiant des droits du tiers bénéficiaire se voient fournir les informations sur leurs droits de tiers bénéficiaire à l'égard du Traitement de leurs Données à caractère personnel et sur les moyens d'exercer ces droits.

À cette fin, les engagements essentiels pris dans le cadre de ces BCR à l'égard des Personnes concernées seront inclus dans une version publique des BCR qui sera publiée sur le site web du Groupe Talan www.talan.com d'une manière facilement accessible aux personnes concernées.

Ces engagements, qui seront inclus dans la version publique des BCR, sont les suivants :

- **L'obligation de respecter les BCR** : Article I.3. « Caractère contraignant des BCR » ;
- **Droits des tiers bénéficiaires** : Article IV.2. « Droits des tiers bénéficiaires » ;
- **Responsabilité envers le Responsable de traitement** : Article IV.3 b) « Responsabilité envers le Responsable de traitement » ;
- **Des ressources financières suffisantes pour couvrir l'indemnisation en cas de violation des BCR** : Article IV.3 a) « Responsabilité envers les tiers bénéficiaires » et b) « Responsabilité envers le Responsable de traitement » ;
- **La charge de la preuve incombe à la société et non à l'individu** : Article IV.3 c) « La charge de la preuve » ;
- **L'obligation de tenir un registre de toutes les catégories d'activités de traitement et de mettre en œuvre le principe de protection de la vie privée dès la conception et par défaut** : Articles IV. 4 a) « Registre » et b) « *Privacy by Design* et *by Default* » ;
- **L'existence d'une procédure de traitement des plaintes concernant les BCR** : Article III. 2 « Mécanisme interne de réclamation » et **Annexe 4** « Procédure de traitement des demandes de droits » ;
- **L'obligation de coopérer avec les Autorités de contrôle** : Article IV. 6 « Coopération avec les Autorités de protection des données » ;
- **L'obligation de coopérer avec le Responsable de traitement** : Article IV. 7 « Coopération avec le Responsable de traitement » ;
- **Une description des transferts et du champ d'application matériel couverts par les BCR** : Article I. 2 b) « Champ d'application matériel » et **Annexe 2** « Description générale du champ d'application matériel des BCR » ;
- **Une déclaration sur la portée géographique des BCR** : Article I. 2 a) « Champ d'application géographique » et **Annexe 1** « Liste des Entités Talan liées par les BCR » ;
- **Une description des principes de protection de la vie privée, y compris les règles relatives aux transferts ou aux transferts ultérieurs en dehors de l'UE** : Article II. 2. « Principes relatifs à la protection des données de Talan » ;
- **La liste des entités liées par les BCR** : **Annexe 1** « Liste des Entités Talan liées par les BCR » ;

- **La nécessité d'être transparent lorsque la législation nationale empêche le groupe de se conformer aux BCR** : Article V. 3 « Actions dans le cas où la législation nationale entrave le respect des BCR » et **Annexe 7** « Politiques de gestion des contrôles des autorités compétentes ».

Les Personnes concernées peuvent en toute occasion obtenir, sur demande, une copie des BCR auprès du DPO local, de l'Entité Talan concernée ou du DPO du Groupe Talan.

Par ailleurs, la liste des Entités Talan est publiée sur le site internet du Groupe Talan d'une façon aisément accessible aux Personnes concernées.

14. Mécanisme interne de réclamation

Chaque Entité Talan doit transmettre, dans les meilleurs délais, toute plainte ou demande d'une Personne concernée qu'elle reçoit, au Responsable de traitement. L'Entité Talan concernée attend les instructions du Responsable de traitement sur la manière de procéder, sauf accord contraire entre les parties dans le Contrat de service.

Bien que Talan encourage les Personnes concernées à contacter directement le Responsable de traitement, Talan leur permet tout de même de soumettre toute plainte ou demande par le biais de la procédure interne de gestion des demandes de droits suivante :

- Procédure principale :

  - Talan identifie le Client ou partenaire agissant en tant que Responsable de traitement dans le cadre de la plainte ou demande et transfert la demande au point de contact du Responsable de traitement identifié contractuellement ou à défaut, à un contact actif et qualifié du Responsable de traitement ;
  - Talan met en œuvre tous les moyens raisonnables à sa disposition pour aider le Responsable de traitement à accéder à la plainte ou demande de la Personne concernée.

Si cela est prévu contractuellement, le Responsable de traitement peut demander à Talan de répondre directement à la plainte ou demande de la Personne concernée. Dans ce cas, Talan contacte immédiatement le DPO du Groupe Talan afin qu'il l'assiste pour répondre à la Personne concernée de manière appropriée.

- Procédure lorsque le Responsable de traitement a disparu :

Conformément aux engagements décrits dans les présentes BCR, le Groupe Talan, et donc par extension chacun de ses Employés, met en œuvre tous les moyens possibles, et raisonnables, pour accéder à la plainte ou demande d'une Personne concernée lorsque celle-ci est dans l'impossibilité matérielle de réaliser cette plainte ou demande auprès du Responsable de traitement.

Concrètement, une Personne concernée peut faire valoir certains droits en vertu des BCR, si :

- La Personne concernée ne peut déposer plainte ou faire une demande auprès du Responsable de traitement parce que celui-ci a matériellement disparu, a cessé d'exister juridiquement, et
- Les obligations juridiques du Responsable de traitement n'ont pas été transférées en totalité, par contrat ou par effet de la loi, à une autre entité lui ayant succédé et auprès de laquelle la Personne concernée peut faire valoir ses droits, et
- La Personne concernée peut démontrer qu'elle a subi des dommages et que ceux-ci résultent probablement d'une violation des BCR.

Lorsqu'une Entité Talan reçoit une telle plainte ou demande, elle la fait remonter immédiatement auprès du DPO du Groupe Talan, conformément à la procédure de gestion des demandes de droits établie par Talan.

Dès réception de la plainte ou demande, le DPO du Groupe Talan peut, en cas de doute raisonnable, procéder à la vérification de l'identité de la Personne concernée.

Le DPO du Groupe Talan se chargera d'informer la Personne concernée de ses droits et des modalités d'exercice de ces droits par l'envoi d'une notice d'information spécifique comprenant notamment les éléments suivants :

- Le DPO du Groupe Talan est le point de contact auquel la plainte ou la demande doit être envoyée par voie électronique à l'adresse dpo@talan.com ;
- La plainte ou la demande est traitée sans délai excessif et, en tout état de cause, dans un délai d'un mois par le DPO du Groupe Talan. Compte tenu de la complexité et du nombre des plaintes ou des demandes, ce délai peut être prolongé de deux mois supplémentaires au maximum, auquel cas la Personne concernée doit être informée en conséquence, sans retard excessif et en tout état de cause dans un délai d'un mois par le DPO du Groupe Talan, en indiquant les raisons du retard ;
- Si la plainte ou la demande est rejetée comme étant injustifiée, le DPO du Groupe Talan enverra à la Personne concernée une notification de refus ;
- Si la plainte ou la demande est jugée justifiée, le DPO du Groupe Talan y donnera suite ;
- Si la Personne concernée n'est pas satisfaite de la réponse du DPO du Groupe Talan, elle a le droit d'introduire une réclamation auprès de l'Autorité de contrôle compétente et/ou des tribunaux compétents ;
- Si le DPO du Groupe Talan ne donne pas suite à la plainte ou à la demande dans les délais impartis, la Personne concernée a le droit de déposer une plainte auprès de l'Autorité de contrôle compétente et/ou des tribunaux compétents.

En sus de l'enregistrement de la demande, le DPO du Groupe Talan complétera et conservera un formulaire récapitulatif de la demande.

15. Sécurité et confidentialité

La protection des Données à caractère personnel contre les atteintes à la sécurité des données constitue l'une des priorités de Talan. Par conséquent :

iv. Chaque Entité Talan est tenue de traiter les Données à caractère personnel pour le compte du Responsable de traitement uniquement, en se conformant à ses instructions et aux mesures de sécurité et de confidentialité prévues par le Contrat de service.

v. Chaque Employé est tenu de traiter les Données à caractère personnel pour le compte du Responsable de traitement uniquement, en se conformant à ses instructions et aux mesures de sécurité et de confidentialité prévues par le Contrat de service.

vi. Chaque Entité Talan doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les Données à caractère personnel contre la destruction fortuite ou illicite, la perte fortuite, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de Traitement illicite. Ces mesures doivent assurer, compte tenu de l'état des connaissances et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le Traitement et de la nature des données à protéger.

Par conséquent, Talan doit garantir la sécurité des informations grâce à la mise en place, au sein du Groupe, de politiques et procédures appropriées, fixant l'ensemble des mesures physiques et logiques nécessaires pour empêcher la destruction ou la modification fortuite des Données à caractère

personnel, ou toute diffusion ou accès non autorisé. Ces politiques et procédures doivent faire l'objet d'audits réguliers conformément à l'Article III.5.

Les Données sensibles doivent faire l'objet de mesures de sécurité renforcées et spécifiques.

L'accès aux Données à caractère personnel est limité aux Destinataires, dans la seule mesure nécessaire à l'exécution de leurs obligations professionnelles. Les Employés qui ne respectent pas les politiques et procédures applicables en matière de sécurité des informations peuvent faire l'objet de sanctions disciplinaires.

16. Programme de formation

Une formation adéquate sur les BCR doit être dispensée aux Employés ayant accès en permanence ou régulièrement aux Données à caractère personnel et associés à la collecte des Données à caractère personnel ou au développement d'outils utilisés pour traiter de telles données.

A cet égard, Talan a créé et mis en œuvre un programme obligatoire et actualisé de formation à la protection des Données à caractère personnel, à l'attention des Employés, qui doit être suivi tous les deux ans.

L'objectif de ce programme de formation est de s'assurer que tous les Employés connaissent et comprennent les principes et les exigences en matière de protection des données, ainsi que l'objectif et le contenu des présentes BCR.

Les Employés reçoivent une formation adaptée à leurs fonctions et responsabilités au sein de Talan leur permettant de traiter les Données à caractère personnel conformément aux principes des BCR.

Ce programme de formation couvre, notamment mais pas exclusivement, la procédure de gestion de demande de divulgation de Données à caractère personnel d'une autorité répressive ou d'un organisme étatique de sécurité et comprend un questionnaire sur les BCR obligatoire pour tous les Employés des Entités Talan. L'accomplissement et le taux de réussite de ce questionnaire sont contrôlés par le manager de l'Employé concerné et globalement par le DPO du Groupe Talan.

En outre, le DPO du Groupe Talan ou les DPO locaux peuvent proposer un programme de formation aux Employés, indépendamment du programme de formation susmentionné, chaque fois qu'ils le jugent nécessaire, notamment mais pas exclusivement, à la suite d'une violation de données ou en cas de modification de la Loi applicable.

17. Audit

Le Groupe Talan a l'obligation de faire réaliser des audits en matière de protection des Données à caractère personnel à intervalles réguliers ou sur demande expresse du DPO du Groupe Talan, par le département d'audit de Talan ou par des auditeurs externes accrédités pour assurer la vérification du respect des BCR.

A cet égard, Talan a défini des politiques internes relatives i) à l'existence d'un programme d'audit couvrant tous les aspects des BCR, y compris les moyens de s'assurer que les actions correctives seront mises en œuvre ii) à la gestion des contrôles des autorités compétentes prévoyant les conditions et modalités dans lesquelles se déroulent les audits relatifs aux BCR.

Ces politiques internes d'audit sont applicables à toutes les Entités Talan.

Ces politiques internes sont décrites à l'**Annexe 5**.

Audit BCR annuel

La politique interne de Talan relative à l'audit et au contrôle du respect des BCR prévoit notamment un contrôle annuel du respect par les Entités Talan des engagements prévus au titre des BCR.

Les résultats d'audit et de contrôle sont communiqués dans un rapport adressé au DPO du Groupe Talan, au DPO local, à la direction du Groupe Talan et à la direction des Entités Talan concernées. Ils sont également rendus accessibles au Responsable de traitement.

Audit sur demande d'un Responsable de traitement

En tant que Sous-traitant, chaque Entité Talan accepte d'être auditée et s'engage, le cas échéant, à ce que tout sous-traitant ultérieur interne ou externe accepte d'être audité sur demande d'un Responsable de traitement en ce qui concerne les activités de Traitement spécifiques effectuées pour son compte.

Ledit audit est réalisé conformément aux dispositions contractuelles convenues entre le Responsable de traitement et l'Entité Talan concernée. L'audit est mené par le Responsable de traitement ou par un organisme d'inspection composé de membres indépendants et en possession des qualifications professionnelles requises, liés par une obligation de confidentialité et sélectionnés par le Responsable de traitement, le cas échéant, en accord avec l'Autorité de contrôle.

Audit sur demande d'une Autorité de contrôle

Sur demande auprès d'une Entité Talan, une Autorité de contrôle compétente peut avoir accès aux résultats des audits annuels relatifs au respect des BCR et/ou de tout audit diligenté à la demande spécifique du DPO du Groupe Talan et/ou de tout audit réalisé par un Responsable de traitement.

Par ailleurs, toute Autorité de contrôle compétente a le pouvoir de réaliser un contrôle sur la protection des données mise en œuvre par une Entité Talan, si nécessaire.

Audit à la demande spécifique du DPO

Le DPO du Groupe Talan peut, à la suite d'une alerte interne ou externe, à la demande d'un DPO local ou à sa propre discrétion, demander un audit (i) de la conformité aux BCR et (ii) des règles mises en œuvre pour assurer la protection des Données à caractère personnel par l'Entité Talan concernée. Les résultats de l'audit sont communiqués dans un rapport à une autorité de contrôle à sa demande, au DPO local, à la direction du Groupe Talan et à la direction de l'entité du Groupe Talan concernée. Ils sont également mis à la disposition du Responsable de traitement.

X. OPPOSABILITÉ DES BCR

18. Respect des BCR et contrôle de leur application par le réseau de délégués à la protection des données du Groupe Talan

Afin de contrôler le respect des BCR, un réseau de DPO a été mis en place au sein du Groupe Talan.

Talan s'engage à nommer, au sein de chaque Entité Talan, des Employés dotés des compétences appropriées et bénéficiant du soutien de la direction, afin de contrôler le respect des BCR adoptées par Talan.

Les DPO qui font partie de l'organisation de gouvernance RGPD, contrôlent la conformité juridique de Talan avec la Loi applicable, donnent des conseils sur toutes les questions relatives à la protection des Données à caractère personnel, mettent en œuvre le programme global de protection des données, traitent les Violations de Données à caractère personnel ou donnent des conseils à ce sujet et entretiennent une relation active avec l'Autorité de contrôle locale.

Plus particulièrement, le DPO du Groupe Talan est chargé de faire respecter l'application des BCR auprès de chacune des Entités Talan.

Les DPO locaux sont désignés par le DPO du Groupe Talan. Les personnes désignées doivent disposer d'une visibilité sur les projets de l'Entité Talan concernée par leur nomination.

Les DPO locaux doivent rapporter annuellement au DPO du Groupe Talan sur les questions principales relatives à la protection des Données à caractère personnel et plus spécifiquement sur le respect des BCR au niveau local et contrôler la formation au niveau local.

Dans le cadre de la fonction juridique, le DPO du Groupe Talan ainsi que les DPO régionaux et locaux sont soutenus dans leur tâche par les équipes juridiques locales et la plus haute direction.

19. Droits des tiers bénéficiaires

En tant que tiers bénéficiaires, les Personnes concernées peuvent faire appliquer les dispositions suivantes des BCR à Talan, agissant en tant que Sous-traitant :

- L'obligation pour les Entités Talan et leurs Employés de respecter les instructions du Responsable de traitement concernant le Traitement des données, y compris dans le cadre des transferts de Données à caractère personnel vers un pays tiers comme détaillé à l'Article IV.3 b) ci-après ;
- L'obligation pour les Entités Talan de mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées, comme indiqué à l'Article III.3 ;
- L'obligation pour les Entités Talan de notifier le Responsable de traitement en cas de Violation de Données à caractère personnel, comme indiqué à l'Article II.2. d) ;
- L'obligation de respecter les conditions d'engagement d'un Sous-traitant à l'intérieur ou à l'extérieur du groupe, comme indiqué à l'Article II.2. f) et g) ;
- L'obligation pour les Entités Talan de coopérer avec le Responsable de traitement et de l'aider à se conformer et à démontrer sa conformité au RGPD, comme détaillé à l'Article IV. 7 ;
- L'obligation pour Talan de faciliter l'accès aux BCR, comme détaillé à l'Article III.1 ;
- Le droit pour les Personnes concernées de faire une réclamation par le biais du mécanisme de réclamation interne de Talan comme détaillé à l'Article III.2 ;
- L'obligation pour les Entités Talan de coopérer avec les Autorités de contrôle compétentes, comme prévu à l'Article IV. 6 ;
- Le droit pour les Personnes concernées de déposer une plainte devant l'Autorité de contrôle compétente et/ou devant les tribunaux compétents, comme détaillé à l'Article IV.3 a) ;
- L'obligation pour chaque Entité Talan exportant des Données à caractère personnel en dehors de l'EEE, d'accepter la responsabilité de toute violation aux BCR par les sous-traitants ultérieurs, Entités Talan non EEE ou sous-traitants externes à Talan établis en dehors de l'EEE, qui ont reçu les Données à caractère personnel, comme détaillé à l'Article IV.3 a) ;
- Le fait qu'il incombe à l'Entité Talan de l'EEE, qui a exporté les Données à caractère personnel, de démontrer que l'Entité Talan non EEE agissant en tant que sous-traitant ultérieur ou tout sous-traitant ultérieur externe établi en dehors de l'EEE, Destinataire des données, n'a pas enfreint les BCR, comme indiqué à l'Article IV.3 c) ;

- Le droit pour les Personnes concernées de se prévaloir des BCR en tant que tiers bénéficiaires dans les situations où elles ne peuvent pas introduire une réclamation contre le Responsable de traitement parce que celui-ci a matériellement disparu, a cessé d'exister juridiquement ou est devenu insolvable, à moins qu'aucune entité lui succédant n'assume l'intégralité des obligations légales du Responsable de traitement par contrat ou par effet de la loi, auquel cas les Personnes concernées peuvent se prévaloir de leurs droits auprès d'une telle entité comme prévu à l'Article III. 2 ;
- L'obligation pour les Entités Talan, et leurs Employés, de respecter les BCR telles que détaillées à l'Article I.3 a) et b) ;
- L'obligation pour Talan de créer des droits de tiers bénéficiaires pour les Personnes concernées, comme détaillé dans ce même Article ;
- Les principes de protection des données énumérés à l'Article II.2 ;
- L'obligation pour chaque Entité Talan de notifier le Responsable de traitement concerné, le DPO du Groupe Talan et le DPO local le cas échéant et l'Autorité de contrôle dont relève le Responsable de traitement et l'Autorité de contrôle dont relève l'Entité Talan concernée, en cas de conflit entre la législation locale et les BCR, comme détaillé à l'Article V.3 ;
- L'obligation de lister les Entités Talan, telles que détaillées en **Annexe 1** et présentées sur le site internet de Talan.

20. Responsabilité et voies de recours

d) Responsabilité envers les tiers bénéficiaires

Comme indiqué à l'Article IV.2, une Personne concernée peut faire valoir certains droits en vertu des BCR en qualité de tiers bénéficiaire, si :

iii) la Personne concernée n'est pas en mesure d'introduire une plainte contre le Responsable de traitement parce que celui-ci a matériellement disparu, a cessé d'exister juridiquement ou est devenu insolvable, et ;

iv) les obligations juridiques du Responsable de traitement n'ont pas été transférées en totalité, par contrat ou par effet de la loi, à une autre entité lui ayant succédé et auprès de laquelle la Personne concernée peut faire valoir ses droits.

Dans ce cas, les Personnes concernées doivent au moins pouvoir faire valoir les droits suivants à l'encontre de Talan agissant en tant que Sous-traitant :

- L'obligation pour les Entités Talan et leurs employés de respecter les instructions du Responsable de traitement concernant le traitement des Données à caractère personnel, y compris pour les transferts de Données à caractère personnel vers un pays tiers, comme indiqué à l'Article IV.3 b) ci-dessous ;
- L'obligation pour les Entités Talan de mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées, comme indiqué à l'Article III.3 ;
- L'obligation de respecter les conditions d'engagement d'un Sous-traitant à l'intérieur ou à l'extérieur du groupe, comme indiqué à l'Article II.2. f) et g) ;
- L'obligation pour Talan de faciliter l'accès aux BCR, comme indiqué à l'Article III.1 ;
- Le droit des Personnes concernées de déposer une plainte par le biais des mécanismes de plainte internes de Talan, tels que décrits à l'Article III.2 ;
- L'obligation pour les Entités Talan de coopérer avec les Autorités de contrôle compétentes, conformément à l'Article IV.6 ;
- Le droit des Personnes concernées d'introduire une réclamation auprès de l'Autorité de contrôle compétente et/ou des tribunaux compétents, comme indiqué à l'Article IV, paragraphe 3, point a) ;

- L’obligation pour chaque Entité Talan exportant des Données à caractère personnel en dehors de l'EEE d'endosser la responsabilité de toute violation des BCR par les sous-traitants ultérieurs, les Entités Talan n'appartenant pas à l'EEE ou les sous-traitants ultérieurs externes établis en dehors de l'EEE, qui ont reçu les Données à caractère personnel, comme indiqué à l'Article IV.3 a) ;
- Le fait qu'il incombe à l'Entité Talan de l'EEE, qui a exporté les Données à caractère personnel, de démontrer que l'Entité Talan hors EEE agissant en tant que sous-traitant ultérieur ou tout sous-traitant ultérieur externe établi en dehors de l'EEE, destinataire des données, n'a pas enfreint les BCR, comme indiqué à l'Article IV.3(c) ;
- Le droit des Personnes concernées de s'appuyer sur les BCR en tant que tiers bénéficiaires lorsqu'elles ne peuvent pas intenter une action contre le Responsable de traitement parce que ce dernier a matériellement disparu, a cessé d'exister juridiquement ou est devenu insolvable, à moins qu'aucune entité succédant au Responsable de traitement des données n'assume toutes les obligations légales de ce dernier par contrat ou par effet de la loi, auquel cas les Personnes concernées peuvent faire valoir leurs droits à l'encontre de cette entité comme prévu à l'Article III. 2 ;
- L’obligation pour les Entités Talan, et leurs Employés, de se conformer aux BCR telles que détaillées à l'Article I.3 a) et b) ;
- L'obligation de Talan de créer des droits de tiers bénéficiaires pour les Personnes concernées, comme indiqué dans ce même article ;
- Les principes de protection des données énumérés à l'Article II.2 ;
- L’obligation pour les entités Talan de notifier le DPO du Groupe Talan et le DPO local, le cas échéant, ainsi que l'Autorité de contrôle dont relève le Responsable de traitement et l'Autorité de contrôle dont relève l'Entité Talan concernée, en cas de conflit entre le droit local et les BCR, comme indiqué à l'Article V.3 ;
- L'obligation de répertorier les Entités Talan, telle que détaillée dans l'**Annexe 1** et présentée sur le site Web de Talan.

Lorsque l'Article IV.2 s'applique, les Personnes concernées disposent de recours juridictionnels en cas de manquement aux droits des tiers bénéficiaires garantis, ainsi que du droit d'obtenir réparation et, le cas échéant, d'être indemnisées pour tout dommage (matériel et moral). En particulier, les Personnes concernées peuvent introduire une réclamation auprès de l'Autorité de contrôle compétente (choix entre l'Autorité de contrôle de l'État membre de sa résidence habituelle, de son lieu de travail ou du lieu de la violation alléguée) et auprès de la juridiction compétente de l'État membre (choix pour la Personne concernée d'agir devant les juridictions du lieu où le Responsable de traitement ou le Sous-traitant a un établissement ou, du lieu où la Personne concernée a sa résidence habituelle). Toute alternative plus favorable aux Personnes concernées en vertu du droit national s'applique.

Lorsque Talan agissant en tant que Sous-traitant et le Responsable de traitement impliqué dans le même Traitement sont jugés responsables de tout dommage causé par ce Traitement, la Personne concernée a le droit de recevoir une compensation pour l'ensemble du dommage directement de Talan agissant en tant que Sous-traitant.

Chaque Entité Talan est responsable de ses propres actes commis en violation des BCR.

Toutefois, chaque Entité Talan de l’EEE exportant des Données à caractère personnel en dehors de l’EEE est responsable des violations des BCR commises par les Entités Talan non EEE et les sous-traitants ultérieurs externes établis en dehors de l’EEE qui ont reçu les Données à caractère personnel de cette Entité Talan dans le cas où ces Entités Talan non EEE ou ces sous-traitants ultérieurs externes établis en dehors de l’EEE seraient incapables de payer lesdites indemnités ou de se conformer à la règle, ou peu disposés à le faire.

Dans un tel cas, l'Entité Talan de l'EEE exportatrice concernée s'engage à prendre les mesures nécessaires afin de remédier aux violations causées, et à verser une réparation au titre des dommages résultant de manquements aux BCR.

La responsabilité de l'Entité Talan de l'EEE exportatrice concernée sera alors engagée dans la même mesure que si le manquement avait été commis par elle dans l'État membre de l'EEE dans lequel elle est domiciliée, plutôt que par l'Entité Talan non EEE ou le sous-traitant ultérieur externe établi en dehors de l'EEE.

L'Entité Talan de l'EEE exportatrice concernée ne peut se décharger de sa responsabilité en invoquant un manquement de l'Entité Talan non EEE ou du sous-traitant ultérieur externe.

Chaque Entité Talan doit disposer de ressources financières suffisantes pour couvrir le dédommagement de la violation des BCR.

e) Responsabilité envers le Responsable de traitement

Les BCR sont contraignantes relativement au Responsable de traitement. À cette fin, les BCR sont intégrées par une référence spécifique à cet aspect, avec possibilité de consultation par voie électronique, dans le Contrat de service, qui satisfait l'article 28 du RGPD.

Le Responsable de traitement a le droit de se prévaloir des BCR auprès de toute Entité Talan concernant une violation qu'elle aurait causée et, auprès de toute Entité Talan de l'EEE exportatrice concernée en cas de violation des BCR ou du Contrat de service par des Entités Talan non EEE ou de violation du Contrat de service par tout sous-traitant ultérieur externe établi en dehors de l'EEE.

Chaque Entités Talan est responsable de ses propres actes commis en violation des BCR.

Toutefois, chaque Entité Talan de l'EEE exportant des Données à caractère personnel en dehors de l'EEE est responsable des violations des BCR commises par les Entités Talan non EEE et les sous-traitants ultérieurs externes établis en dehors de l'EEE qui ont reçu les Données à caractère personnel de cette Entité Talan dans le cas où ces Entités Talan non EEE ou ces sous-traitants ultérieurs externes établis en dehors de l'EEE seraient incapables de payer lesdites indemnités ou de se conformer à la règle, ou peu disposés à le faire.

Dans un tel cas, l'Entité Talan de l'EEE exportatrice concernée s'engage à prendre les mesures nécessaires afin de remédier aux violations causées, et à verser une réparation au titre des dommages résultant de manquements aux BCR.

La responsabilité de l'Entité Talan de l'EEE exportatrice concernée sera alors engagée dans la même mesure que si le manquement avait été commis par elle dans l'État membre de l'EEE dans lequel elle est domiciliée, plutôt que par l'Entité Talan non EEE ou le sous-traitant ultérieur externe établi en dehors de l'EEE.

L'Entité Talan de l'EEE exportatrice concernée ne peut se décharger de sa responsabilité en invoquant un manquement de l'Entité Talan non EEE ou du sous-traitant ultérieur externe.

Chaque Entité Talan doit disposer de ressources financières suffisantes pour couvrir le dédommagement de la violation des BCR.

f) La charge de la preuve

Il incombe à l'Entité Talan de l'EEE exportatrice concernée d'endosser la responsabilité de prouver que l'Entité Talan non EEE ou le sous-traitant ultérieur externe établi en dehors de l'EEE n'est responsable d'aucune violation des règles ayant entraîné une demande de réparation de la part de la Personne concernée.

Si le Responsable de traitement peut démontrer qu'il a subi des préjudices et présenter des faits montrant que ces préjudices ont probablement été causés par une violation des BCR, il incombe à l'Entité Talan de l'EEE exportatrice concernée de prouver que l'Entité Talan non EEE ou le sous-traitant ultérieur externe établi en dehors de l'EEE n'est pas responsable de la violation des BCR entraînant ces préjudices ou que ladite violation n'a pas eu lieu. L'Entité Talan de l'EEE exportatrice concernée peut être exonérée de toute responsabilité si elle est en mesure de prouver que l'Entité Talan non EEE ou le sous-traitant ultérieur externe établi en dehors de l'EEE n'est pas responsable de l'acte.

21. *Accountability* et autres outils

En tant que Sous-traitant, Talan doit fournir au Responsable de traitement toutes les informations nécessaires pour démontrer le respect de ses obligations.

p) Registre

Les Entités Talan sont tenues de conserver et tenir à jour, par écrit, y compris sous forme électronique, un registre de toutes les catégories d'activités de Traitement effectuées pour le compte des Responsables de traitement, comportant les éléments suivants :

- Le nom et les coordonnées de l'Entité Talan agissant en tant que Sous-traitant, et de chaque Responsable de traitement pour le compte duquel Talan agit, ainsi que le DPO ;
- Les catégories de Traitement effectuées pour le compte du Responsable de traitement ;
- Le cas échéant, les Transferts de Données à caractère personnel vers des pays situés en dehors de l'EEE y compris l'identification de ces pays ;
- Dans la mesure du possible, une description générale des mesures techniques et organisationnelles mises en œuvre.

Talan doit mettre le dossier à la disposition de l'Autorité de contrôle compétente sur demande.

q) AIPD

Les Entités Talan sont tenues d'aider le Responsable de traitement à se conformer à son obligation d'effectuer des AIPD pour les Traitements susceptibles d'engendrer un risque élevé pour les droits et les libertés des Personnes concernées.

Dans le cas où de telles AIPD sont réalisées, les Entités Talan doivent fournir au Responsable de traitement toutes les informations pertinentes concernant le Traitement, en particulier, les moyens techniques et organisationnels utilisés pour mettre en œuvre le Traitement, la localisation des Données à caractère personnel, les mesures de sécurité mises en œuvre (physiques et techniques), et si applicable, les détails sur le(s) sous-traitant(s) ultérieur(s) etc.

Toutefois, les Entités Talan ne sont pas tenues de mener d'AIPD pour le compte du Responsable de traitement. Les Entités Talan ne font qu'assister les Responsables de traitement sans s'engager sur l'exécution de l'AIPD en tant que telle.

r) *Privacy by Design* et *by Default*

Talan s'engage à respecter les principes relatifs à la protection des données énoncés dans les présentes BCR, indépendamment de la Loi applicable, sauf si la Loi applicable prévoit des exigences plus strictes que celles énoncées dans ces BCR.

Les Entités Talan s'engagent à aider le Responsable de traitement à mettre en œuvre les mesures techniques et organisationnelles appropriées pour respecter les principes de protection des données et faciliter le respect des exigences établies par les BCR en pratique, telles que la protection des

données dès la conception et par défaut.

À cet égard, lorsqu'elles assistent le Responsable de traitement, les Entités Talan s'engagent, en tenant compte de l'état de la technique, du coût de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du Traitement, ainsi que des risques de probabilité et de gravité variables pour les droits et libertés des personnes physiques que présente le Traitement, tant au moment de la détermination des moyens de traitement qu'au moment du Traitement lui-même, de s'efforcer raisonnablement de mettre en œuvre de manière efficace les mesures techniques et organisationnelles appropriées, conçues pour appliquer les principes de protection des données, et d'intégrer les garanties nécessaires dans le Traitement afin de satisfaire aux exigences des présentes BCR et de protéger les droits des Personnes concernées.

En outre, lorsqu'elles assistent le Responsable de traitement, les Entités Talan s'engagent à mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les Données à caractère personnel qui sont nécessaires pour chaque finalité spécifique du Traitement soient traitées. Cette obligation s'applique à la quantité de Données à caractère personnel collectées, à l'étendue de leur Traitement, à la durée de leur conservation et à leur accessibilité.

Par ailleurs, Talan s'engage à promouvoir la mise en œuvre de ces principes au sein de l'organisation du Groupe Talan par le biais de ses politiques internes, notamment des formations à destination des Employés et des actions de communication dédiées à la sensibilisation aux principes relatifs à la protection des données au sein des Entités Talan.

22. Sanctions

Toute violation des BCR par un représentant ou un Employé d'une Entité Talan peut donner lieu à des sanctions disciplinaires ou à des poursuites judiciaires, conformément au droit du travail applicable, sur décision de Talan, du DPO du Groupe Talan, de l'Entité Talan concernée ou du DPO local.

Par conséquent, l'Entité Talan et le DPO local doivent prêter une attention particulière à tout résultat d'audit laissant apparaître des problèmes de conformité concernant certains représentants ou Employés, notamment les problèmes suivants :

- La violation des principes relatifs à la protection des données énoncés à l'Article II.2 ;
- La violation des politiques de sécurité conçues en vue de la mise en œuvre de mesures techniques et organisationnelles appropriées, destinées à protéger les Données à caractère personnel ;
- Le non-respect des obligations relatives aux programmes de formation destinés à sensibiliser les Employés aux questions et principes relatifs à la protection des données.

23. Coopération avec les Autorités de protection des données

Toute Entité Talan doit coopérer avec la ou les Autorités de contrôle compétentes pour le Responsable de traitement.

En particulier, les Entités Talan prendront en compte l'avis des Autorités de contrôle compétentes, accepteront d'être contrôlées par ces Autorités de contrôle et se conformeront aux décisions de ces Autorités de contrôle sur toute question liée aux BCR.

Les Entités Talan s'engagent à fournir aux Autorités de contrôle compétentes, sur demande, toute information sur les opérations de traitement couvertes par les BCR.

Tout litige lié à l'exercice du contrôle du respect des BCR par une Autorité de contrôle compétente sera

résolu par les tribunaux de l'État membre de cette Autorité de contrôle, conformément au droit procédural de cet État membre. Les Entités Talan acceptent de se soumettre à la juridiction de ces tribunaux.

24. Coopération avec le Responsable de traitement

Toute Entité Talan doit coopérer avec le Responsable de traitement et l'assister pour l'aider à se conformer à ses obligations en vertu de la Loi applicable.

Cette obligation doit être respectée dans un délai raisonnable et dans la mesure où cela est raisonnablement possible.

XI. STIPULATIONS FINALES

25. Liens entre la législation nationale et les BCR

Talan s'engage à faire en sorte que les Entités Talan et les Employés concernés du Groupe respectent les BCR ainsi que la Loi applicable.

Si la législation locale exige un degré supérieur de protection des Données à caractère personnel, celle-ci prime sur les BCR.

26. Transferts ultérieurs vers des sous-traitants ultérieurs externes

Lorsqu'une Entité Talan demande à une entité ne faisant pas partie du Groupe de traiter des Données à caractère personnel, les garanties suivantes doivent être mises en place :

iv) Lorsqu'une Entité Talan sous-traite les obligations qui lui incombent en vertu du Contrat de service à un sous-traitant ultérieur externe établi dans l'EEE ou dans un pays reconnu par la Commission européenne comme garantissant un niveau adéquat de protection, le sous-traitant ultérieur externe est lié par contrat écrit stipulant que le sous-traitant ultérieur n'agit que sur seule instruction de l'Entité Talan concernée et est responsable de la mise en œuvre des mesures de sécurité et de confidentialité adéquates telles que prévues à l'Article III.3 ;

v) Les DPO locaux doivent pouvoir fournir, en coordination avec le DPO du Groupe Talan, les Clauses types de l'UE aux Entités Talan ;

vi) Lorsqu'une Entité Talan sous-traite les obligations qui lui incombent en vertu du Contrat de service à un sous-traitant ultérieur externe établi en dehors de l'EEE avec le consentement du Responsable de traitement, il est tenu de signer un contrat écrit avec le sous-traitant ultérieur afin de garantir un niveau de protection adéquat, conformément au Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, et d'imposer au sous-traitant ultérieur les mêmes obligations que celles qui lui incombent en vertu du Contrat de service ainsi que des Articles IV.2,3,4,5,6 et 7 des BCR.

27. Actions dans le cas où la législation nationale entrave le respect des BCR

Lois et pratiques locales affectant le respect des BCR

Les Entités Talan s'engagent à utiliser ces BCR comme outil pour les Transferts uniquement lorsqu'elles ont évalué que le droit et les pratiques du pays tiers de destination applicables au Traitement des Données à caractère personnel par l'Entité Talan agissant en tant qu'importateur de données, y compris toute exigence de divulgation des Données à caractère personnel ou toute mesure autorisant l'accès par les autorités publiques, ne l'empêchent pas de remplir ses obligations en vertu de ces BCR. Il est entendu que les lois et pratiques qui respectent l'essence des droits et libertés fondamentaux et n'excèdent pas ce qui est nécessaire et proportionné dans une société démocratique pour sauvegarder l'un des objectifs énumérés à l'article 23, paragraphe 1, du RGPD, ne sont pas en contradiction avec les BCR.

Les Entités Talan s'engagent à ce que, lors de l'évaluation des lois et pratiques du pays tiers susceptibles d'affecter le respect des exigences contenues dans les BCR, les Entités Talan aient dûment tenu compte, en particulier, des éléments suivants :

i) Les circonstances spécifiques des Transferts ou de l'ensemble des Transferts, et de tout Transfert ultérieur envisagé au sein du même pays tiers ou vers un autre pays tiers, y compris :

- les finalités pour lesquelles les données sont transférées et traitées (par exemple, marketing, RH, stockage, support informatique, essais cliniques) ;
- les types d'entités impliquées dans le Traitement (l'importateur de données et tout autre destinataire d'un Transfert ultérieur) ;
- le secteur économique dans lequel le Transfert ou l'ensemble des Transferts ont lieu ;
- les catégories et le format des Données à caractère personnel transférées ;
- le lieu du Traitement, y compris le stockage ;
- et les canaux de transmission utilisés.

ii) Les lois et pratiques du pays tiers de destination pertinentes à la lumière des circonstances du Transfert, y compris celles exigeant la divulgation des données aux autorités publiques ou autorisant l'accès de ces autorités et celles prévoyant l'accès à ces données pendant le transit entre le pays de l'exportateur de données et le pays de l'importateur de données, ainsi que les limitations et sauvegardes applicables.

iii) Toutes les garanties contractuelles, techniques ou organisationnelles pertinentes mises en place pour compléter les garanties prévues par les présentes BCR, y compris les mesures appliquées lors du Transfert et du traitement des Données à caractère personnel dans le pays de destination.

Si des garanties autres que celles prévues par les BCR doivent être mises en place, la ou les Entités Talan concernées et le DPO local compétent seront informés et associés à cette évaluation.

Les Entités Talan doivent documenter de manière appropriée cette évaluation, ainsi que les mesures supplémentaires sélectionnées et mises en œuvre. Elles doivent mettre cette documentation à la disposition des Autorités de contrôle compétentes qui en font la demande.

Toute Entité Talan agissant en tant qu'importateur de données s'engage à notifier rapidement l'exportateur de données si, lors de l'utilisation de ces BCR en tant qu'outil pour les Transferts, et pendant la durée de l'adhésion aux BCR, elle a des raisons de croire qu'elle est, ou est devenue soumise à des lois ou à des pratiques qui l'empêcheraient de remplir ses obligations en vertu de ces BCR, y compris à la suite d'une modification des lois dans le pays tiers ou d'une mesure (telle qu'une demande de divulgation). Ces informations doivent également être communiquées au Responsable de traitement et à l'Entité Talan concernée.

Après vérification de cette notification, l'Entité Talan agissant en tant qu'exportateur de données, ainsi que la ou les Entités Talan concernées et le DPO local compétent, devraient s'engager à identifier rapidement des mesures supplémentaires (par exemple, des mesures techniques ou organisationnelles visant à garantir la sécurité et la confidentialité) à adopter par l'Entité Talan agissant en tant qu'exportateur et/ou importateur de données, afin de leur permettre de remplir leurs obligations au titre des présentes BCR. Il en va de même si une Entité Talan agissant en tant qu'exportateur de données a des raisons de croire qu'une Entité Talan agissant en tant qu'importateur de données ne peut plus remplir ses obligations au titre des présentes BCR.

Lorsque l'Entité Talan agissant en tant qu'exportateur de données, ainsi que la ou les Entités Talan concernées et le DPO local compétent, estime que les BCR (même si elles sont accompagnées de mesures supplémentaires) ne peuvent pas être respectées pour un Transfert ou un ensemble de Transferts, ou sur instruction de l'Autorité de contrôle compétente, elle s'engage à suspendre le Transfert ou l'ensemble de Transferts en question, ainsi que tous les transferts pour lesquels la même évaluation et le même raisonnement aboutiraient à un résultat similaire, jusqu'à ce que le respect soit à nouveau assuré ou que le Transfert prenne fin.

À la suite d'une telle suspension, l'Entité Talan agissant en tant qu'exportateur de données s'engage à mettre fin au Transfert ou à l'ensemble de Transferts si les BCR ne peuvent pas être respectées et si le respect des BCR n'est pas rétabli dans un délai d'un mois à compter de la suspension. Dans ce cas, les Données à caractère personnel qui ont été transférées avant la suspension, ainsi que toute copie de ces données, doivent, au choix de l'Entité Talan agissant en tant qu'exportateur de données (suivant les instructions du Responsable de traitement des données), lui être renvoyées ou être détruites dans leur intégralité.

La ou les Entités Talan concernées et le DPO local compétent informeront toutes les autres Entités Talan de l'évaluation réalisée et de ses résultats, afin que les mesures supplémentaires identifiées soient appliquées au cas où le même type de Transferts serait effectué par une autre Entité Talan ou, si des mesures supplémentaires efficaces n'ont pas pu être mises en place, que les Transferts en question soient suspendus ou qu'il y soit mis fin.

Les Entités Talan agissant en tant qu'exportateur de données surveillent en permanence, et le cas échéant en collaboration avec les Entités Talan agissant en tant qu'importateur, les développements dans les pays tiers vers lesquels les Entités Talan agissant en tant qu'exportateur de données ont transféré des Données à caractère personnel qui pourraient affecter l'évaluation initiale du niveau de protection et les décisions prises en conséquence sur ces Transferts.

Demande juridiquement contraignante de divulgation de Données à caractère personnel par une autorité chargée de l'application de la loi ou un organisme de sécurité de l'État

L'Entité Talan agissant en tant qu'importateur de données notifiera rapidement à l'exportateur de données si elle :

e) reçoit une demande juridiquement contraignante d'une autorité publique en vertu des lois du pays de destination, ou d'un autre pays tiers, pour la divulgation de Données à caractère personnel transférées conformément aux BCR ; cette notification comprendra des informations sur les Données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse apportée ;

f) prend connaissance de tout accès direct par les autorités publiques aux Données à caractère personnel transférées en vertu des BCR conformément aux lois du pays de destination ; cette notification comprendra toutes les informations dont dispose l'Entité Talan agissant en tant qu'importateur de données.

Ces informations doivent également être communiquées au Responsable de traitement et à l'Entité Talan concernée.

S'il lui est interdit de notifier l'exportateur de données et/ou le Responsable de traitement et/ou la Personne concernée, l'Entité Talan agissant en tant qu'importateur de données fera de son mieux pour obtenir une dérogation à cette interdiction, en vue de communiquer autant d'informations que possible et dans les meilleurs délais, et documentera ses meilleurs efforts afin de pouvoir les démontrer à la demande de l'exportateur de données / du Responsable de traitement.

L'Entité Talan agissant en tant qu'importateur de données fournira à l'exportateur de données / au Responsable de traitement des données, à intervalles réguliers, autant d'informations pertinentes que possible sur les demandes reçues (en particulier, le nombre de demandes, le type de données demandées, l'autorité ou les autorités requérante(s), si les demandes ont été contestées et le résultat de ces contestations, etc.). Si l'Entité Talan agissant en tant qu'importateur de données est ou devient partiellement ou totalement empêchée de fournir à l'exportateur de données / au Responsable de traitement, les informations susmentionnées, elle en informera l'exportateur de données / le Responsable de traitement dans les plus brefs délais.

L'Entité Talan agissant en tant qu'importateur de données conservera les informations susmentionnées aussi longtemps que les Données à caractère personnel seront soumises aux garanties prévues par les BCR, et les mettra à la disposition de l'Autorité ou des Autorités de contrôle compétente(s) sur demande.

L'Entité Talan agissant en tant qu'importateur de données examinera la légalité de la demande de divulgation, en particulier si elle reste dans les limites des pouvoirs accordés à l'autorité publique requérante, et contestera la demande si, après une évaluation minutieuse, elle conclut qu'il existe des motifs raisonnables de considérer que la demande est illégale en vertu des lois du pays de destination, des obligations applicables en vertu du droit international et des règles de la courtoisie internationale.

L'Entité Talan agissant en tant qu'importateur de données poursuivra, dans les mêmes conditions, les possibilités de recours. Lorsqu'elle conteste une demande, l'Entité Talan agissant en tant qu'importateur de données prendra des mesures provisoires en vue de suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente ait statué sur son bien-fondé. Elle ne divulguera pas les Données à caractère personnel demandées tant qu'elle n'y sera pas contrainte par les règles de procédure applicables.

L'Entité Talan agissant en tant qu'importateur de données documentera son évaluation juridique et toute contestation de la demande de divulgation et, dans la mesure où les lois du pays de destination le permettent, mettra la documentation à la disposition de l'exportateur de données / du Responsable de traitement. Elle la mettra également à la disposition de l'Autorité ou des Autorités de contrôle qui en feront la demande.

L'Entité Talan agissant en tant qu'importateur de données fournira la quantité minimale d'informations autorisée lorsqu'elle répondra à une demande de divulgation, sur la base d'une interprétation raisonnable de la demande.

La procédure de traitement des demandes de divulgation de Données à caractère personnel par une autorité chargée de l'application de la loi ou un organe de sécurité de l'État est décrite à l'**Annexe 7**.

En tout état de cause, les transferts de Données à caractère personnel par une Entité Talan à une autorité publique, quelle qu'elle soit, ne sauraient être massifs, disproportionnés et sans distinction, ni aller au-delà de ce qui est nécessaire dans une société démocratique.

28. Mise à jour des BCR

En cas de modification de la loi applicable ou des procédures de Talan, les dispositions de ces BCR peuvent être modifiées à la discrétion de Talan, en coordination avec le DPO du Groupe Talan.

Le DPO du Groupe Talan gardera trace et enregistrera toute modification, substantielle ou non, des BCR et fournira systématiquement les informations nécessaires aux clients et aux Autorités de contrôle sur demande.

Le DPO du Groupe Talan tient également à jour une liste complète des Entités Talan et des sous-traitants ultérieurs impliqués dans les activités de traitement, accessible aux Clients, aux Personnes concernées et aux Autorités de contrôle.

Talan s'engage à fournir aux Entités Talan, aux Clients et aux Personnes concernées les informations appropriées concernant toute modification des BCR, y compris la liste des Entités Talan, dans les meilleurs délais.

Toute modification des BCR susceptible d'affecter éventuellement de manière significative les BCR ou de nuire au niveau de protection qu'elles offrent, par exemple des modifications du caractère contraignant ou de la liste des Entités Talan, sera communiquée à l'avance aux Autorités de contrôle concernées par l'intermédiaire de l'Autorité chef de file, avec une brève explication des raisons de la mise à jour.

Dans ce cas, Talan s'engage également à informer le Responsable de traitement en temps utile pour que ce dernier ait la possibilité de s'opposer à la modification ou de résilier le Contrat de service avant que la modification ne soit effectuée.

Une fois par an, Talan s'engage à notifier aux Autorités de contrôle compétentes, par l'intermédiaire de l'Autorité chef de file, toute modification apportée aux BCR ou à la liste des Entités Talan, en expliquant brièvement les raisons de ces modifications.

Aucun Transfert ne sera effectué vers une nouvelle Entité Talan tant que cette nouvelle entité ne sera pas effectivement liée par les BCR et ne pourra pas en assurer le respect.

29. Résiliation

Toute Entité Talan agissant en tant qu'importateur de données qui cesse d'être liée par les BCR doit, à la demande du Responsable de traitement, supprimer ou renvoyer toutes les Données à caractère personnel transférées au Responsable de traitement et en supprimer les copies, et certifier au Responsable de traitement qu'elle l'a fait, à moins que la législation qui leur est imposée n'exige le stockage des Données à caractère personnel transférées. Dans ce cas, l'Entité Talan concernée informera le Responsable de traitement et garantira qu'elle assurera la confidentialité des Données à

caractère personnel transférées et qu'elle ne traitera plus activement les Données à caractère personnel transférées.

30. Non-conformité

Les Entités Talan doivent informer rapidement l'exportateur de données / le Responsable de traitement si elles ne sont pas en mesure de se conformer aux BCR, quelle qu'en soit la raison, y compris les situations décrites à l'Article V. 3. des BCR.

Lorsqu'une Entité Talan ne respecte pas les BCR ou n'est pas en mesure de les respecter, l'exportateur de données doit suspendre le Transfert.

L'Entité Talan doit, au choix du Responsable de traitement (et, à défaut, au choix de l'exportateur de données), renvoyer ou supprimer immédiatement les Données à caractère personnel qui ont été transférées en vertu des BCR dans leur intégralité, lorsque :

- le Responsable de traitement et/ou l'exportateur de données a suspendu le transfert et le respect des présentes BCR n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ; ou
- l'Entité Talan enfreint de manière substantielle ou persistante les BCR ; ou
- l'Entité Talan ne se conforme pas à une décision contraignante d'un tribunal compétent ou d'une autorité de surveillance compétente concernant ses obligations au titre des BCR.

Les mêmes engagements s'appliquent à toute copie des données. L'Entité Talan doit certifier la suppression des données à l'exportateur de données / au Responsable de traitement.

Jusqu'à ce que les données soient supprimées ou restituées, l'Entité Talan doit continuer à veiller au respect des BCR.

Si la législation locale applicable à l'Entité Talan interdit la restitution ou la suppression des Données à caractère personnel transférées, l'Entité Talan doit garantir qu'elle continuera à veiller au respect des BCR et qu'elle ne traitera les données que dans la mesure et pour la durée requises par cette législation locale.

XII. Annexes

31. Liste des Entités Talan liées par les BCR
32. Description générale du champ d'application matériel des BCR
33. Modèle de clauses type de protection des données devant être ajoutées aux Contrats de service conclus avec les Clients
34. Procédure de gestion des demandes de droits
35. Politique d'audit et de contrôle du respect des BCR du groupe Talan
36. Politique de gouvernance RGPD
37. Politiques de gestion des contrôles des autorités compétentes

ANNEXE 1 - LISTE DES ENTITES DE TALAN LIEES PAR LES BCR

ZONE GÉOGRAPHIQUE	NB	PAYS	NB	NOM DE L'ENTITÉ	DESCRIPTION DE L'ACTIVITÉ	COORDONNÉES
UNION EUROPÉENNE	9	France	6	Talan Corporate	Talan Corporate est l'entité principale du groupe Talan, elle constitue l'entité décisionnelle et fournit les services de soutien à toutes les entités du groupe (stratégie, finance, juridique, marketing, ressources humaines, informatique, etc.) À ce titre, TALAN CORPORATE a des responsabilités déléguées en matière de protection des données. Le responsable juridique et de la conformité pour la protection des données du groupe est rattaché à cette entité.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 515 132 694 R.C.S. PARIS
				Talan Holding	Talan Holding est la société holding du groupe Talan. Talan Holding n'a pas	Société par actions simplifiée 14-20 rue Pergolèse, 75116

					d'activité commerciale, détient des actions et gère ses filiales.	Paris, FRANCE 887 633 733 R.C.S. PARIS
				Talan SAS	TALAN SAS intervient en France et à l'étranger dans les domaines suivants : Services informatiques, ingénierie, conseil et assistance technique en systèmes d'information.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 488 601 337 R.C.S. PARIS
				Talan Consulting	Conseil en gestion et systèmes d'information.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 481 088 789 R.C.S. PARIS
				Talan LABS	Prestation de services dans le domaine des technologies de l'information, création et édition de logiciels, commercialisation (vente) de matériel et de logiciels.	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 887 633 733 R.C.S. PARIS
				Solutions Talan	Services et expertise, conseil en développement, recherche et ingénierie. L'étude, la conception, la mise en œuvre, le développement de projets informatiques, puis de projets de formation associés. La prise de participation dans toutes les sociétés	Société par actions simplifiée 14-20 rue Pergolèse, 75116 Paris, FRANCE 508 878 386 R.C.S. PARIS

					et la gestion du portefeuille ainsi constitué.	
		Espagne	1	Talan Consulting Espana	Services informatiques et assistance technique	Société à responsabilité limitée inscrite au registre du commerce et des sociétés de Madrid sous le numéro d'identification 97960423 Paseo de la Castellana 200 Madrid 28046, ESPAGNE
		Belgique	1	TALAN Belgique	Services informatiques et assistance technique	Société à responsabilité limitée inscrit au Registre du Commerce et des Sociétés de Bruxelles sous le numéro d'identification 778 693 036 Avenue Arnaud Fraiteur 15 1050 Ixelles, BELGIQUE
		Luxembourg	1	Talan Luxembourg	Services informatiques et assistance technique	Société à responsabilité limitée inscrit au registre du commerce et des sociétés de Luxembourg sous le numéro d'identification 101418 21 rue Glesener 1631 Luxembourg, LUXEMBOURG

L'Europe	3	Royaume-Uni	2	Business Data Partners Ltd	Services informatiques et assistance technique	Société à responsabilité limitée enregistrée en vertu des lois de l'Angleterre et du Pays de Galles auprès de la Companies House sous le numéro d'identification 09277132 28 Lime Street, London, EC3M 7HR - 2nd floor, ROYAUME-UNI
				Talan Consulting UK Ltd	Services informatiques et assistance technique	Société privée à responsabilité limitée enregistrée en vertu des lois de l'Angleterre et du Pays de Galles auprès de la Companies House sous le numéro d'identification 05388143 28 Lime Street, London, EC3M 7HR - 2nd floor, ROYAUME-UNI
		Suisse	1	Talan Suisse	Services informatiques et assistance technique	Société à responsabilité limitée inscrit au registre du commerce et des sociétés de Genève sous le numéro d'identification 106.832.761 Place Ruth-BÖSIGER 6, 1201 Genève, SUISSE
Amérique du NORD	3	Canada	2	Talan Canada Inc	Services informatiques et assistance technique	Société canadienne par actions immatriculée en vertu des lois du Canada au Registre du commerce et des sociétés du Québec sous le numéro d'identification 1163837454 700-60 rue Saint-Jacques

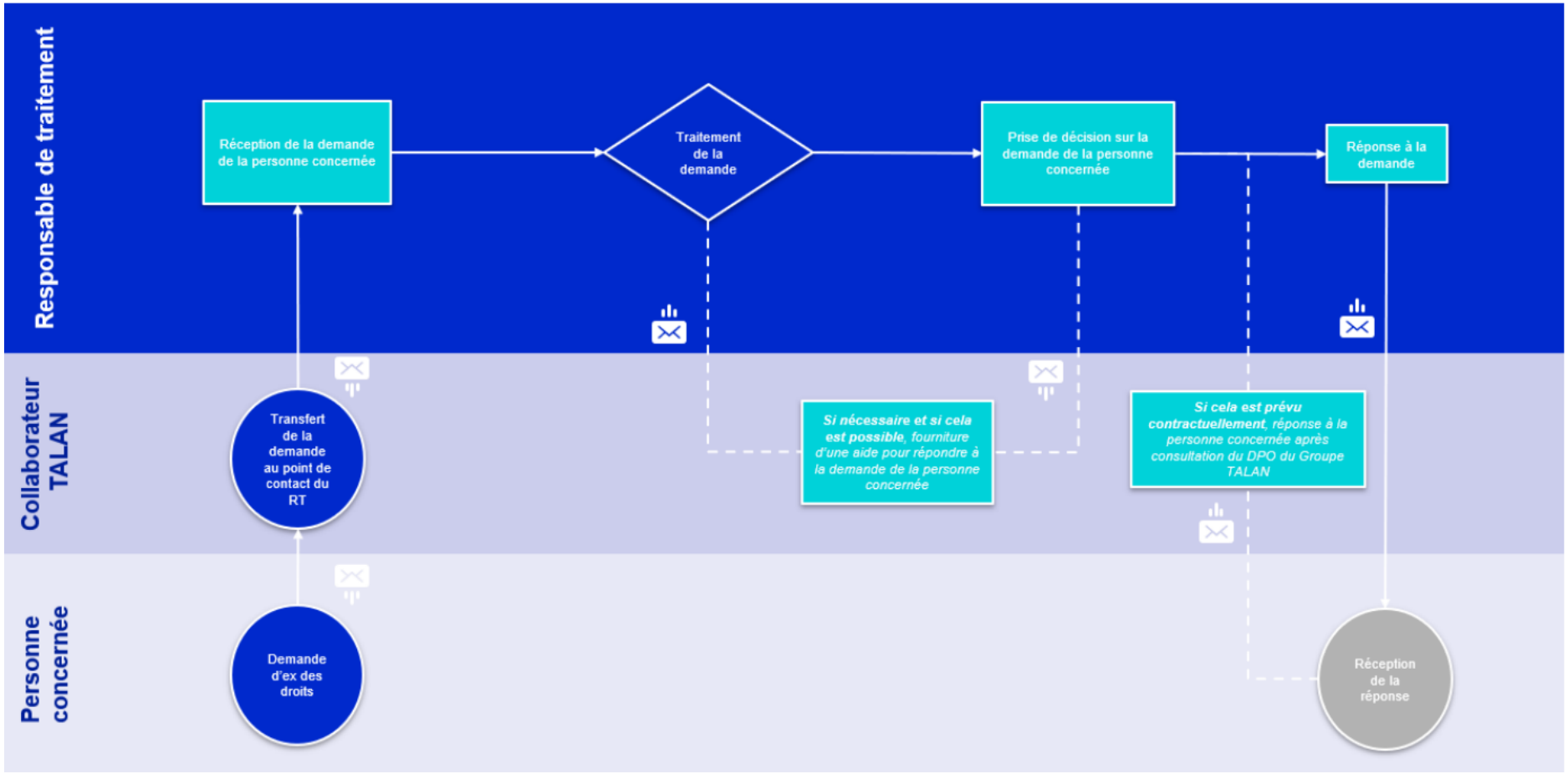
						Montréal, Québec, H2Y1L5, CANADA
				Talan Conseil Canada INC	Services et assistance technique de l'IIT	Société canadienne par actions immatriculée en vertu des lois du Canada au Registre du commerce et des sociétés du Québec sous le numéro d'identification 1169006146 700-60 rue Saint Jacques Montréal, Québec, H2Y1L5, CANADA
		ÉTATS-UNIS	1	Talan LLC	Services informatiques et assistance technique	Société à responsabilité limitée inscrit au registre du commerce et des sociétés du Delaware sous le numéro d'identification 20-4193242 en vertu des lois de l'État du Delaware 33 Irving Place - New York, 10003 New York, USA
Afrique	1	Tunisie	1	Talan Tunisie Consulting	Centre Nearshore qui travaille exclusivement pour les sociétés du Groupe Talan et leurs clients : Développement de logiciels, projets informatiques, Tierce Maintenance Applicative (TMA).	Société à responsabilité limitée inscrite au registre du commerce et des sociétés de Tunis sous le numéro d'identification 1325392 10 rue de l'Energie Solaire, Impasse N°1 2035 Tunis, TUNISIE
TOTAL	16		16			

ANNEXE 2 : DESCRIPTION GENERALE DU CHAMP D'APPLICATION MATERIEL DES BCR

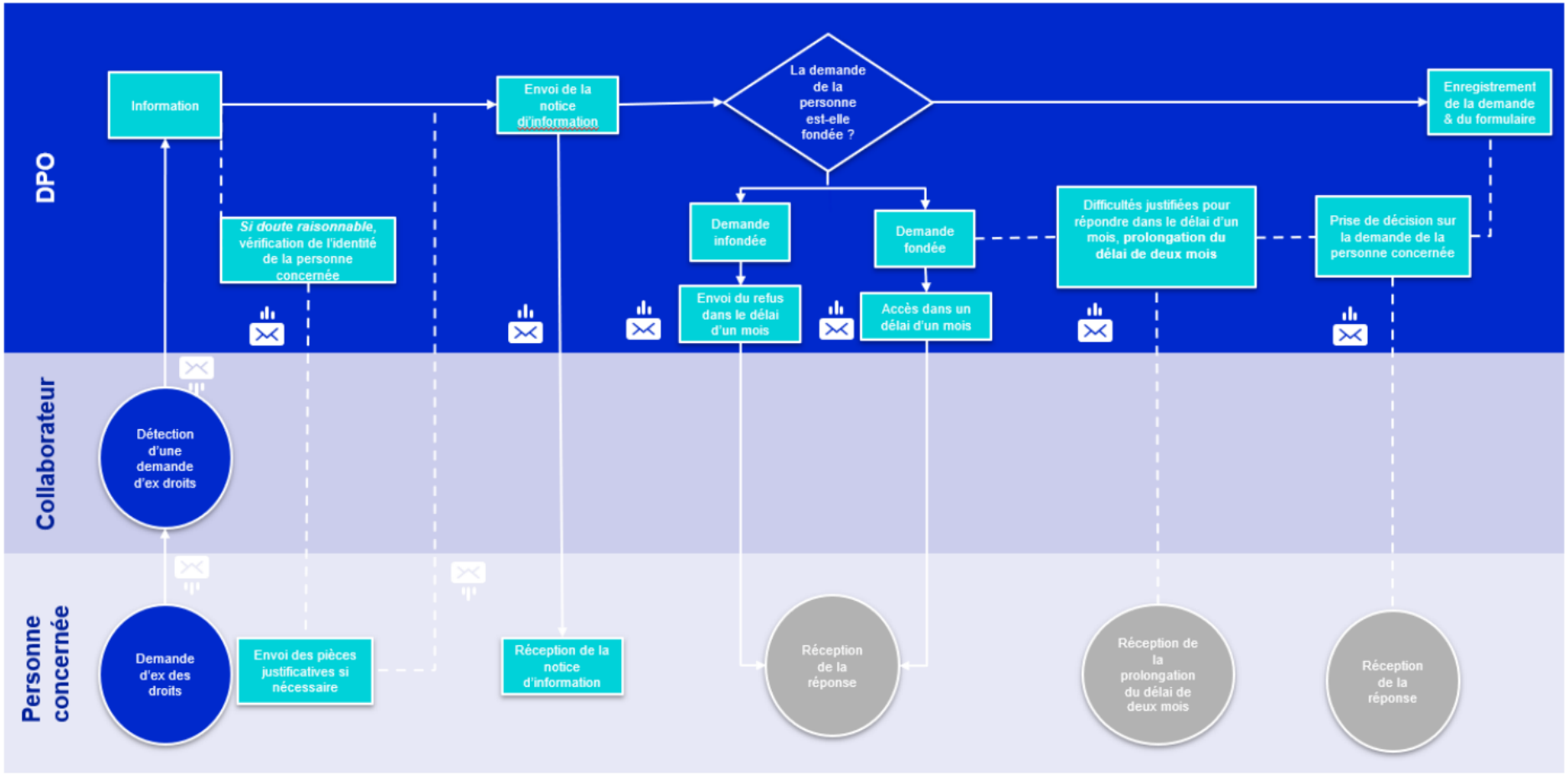
Finalités du transfert de données et du traitement ultérieur	TALAN traite les données personnelles de ses Clients afin de mener à bien leurs projets liés notamment aux services informatiques, au conseil en management, à la création et à l'édition de logiciels, à l'assistance technique, etc. L'objectif du transfert des données personnelles du Client est de permettre à l'entité la plus efficace du Groupe TALAN, en fonction du Client et de la nature des services, de fournir les services convenus avec le Client.
Nature du transfert de données	*TALAN LLC (ÉTATS-UNIS)* Fourniture de services informatiques et d'assistance technique. *TALAN TUNISIE CONSULTING (Tunisie)* : Fourniture de services de développement de logiciels, de services informatiques et d'assistance technique, de maintenance d'applications par des tiers (TPMA).
Catégories de données personnelles transférées	Les catégories de données personnelles traitées par TALAN Group, conformément à la loi applicable, dépendent des services fournis au Client et peuvent inclure, mais ne sont pas limitées à : - des données d'identification ou des informations personnelles (par exemple, les noms, l'adresse, le numéro de téléphone, l'adresse électronique...) - des données relatives à la vie professionnelle (par exemple, la fonction, la société d'affiliation, le contrat de travail, la date d'embauche, le numéro d'identification de l'employé, les coordonnées professionnelles...) - des données économiques et financières (par exemple, les informations fiscales, les coordonnées bancaires...) - des données de localisation (par exemple, les informations d'accès) - des données de connexion et d'utilisation (par exemple, connexions, les adresses IP...).
Types de catégories particulières de données personnelles transférées (le cas échéant)	TALAN peut traiter des données sensibles telles que des informations sur la santé, y compris toute condition médicale, les dossiers de santé et de maladie. Lorsque des données personnelles sensibles sont traitées par le groupe TALAN, conformément à la loi applicable, des mesures supplémentaires s'appliquent.
Catégories de personnes concernées dont les données personnelles sont transférées	Les catégories de personnes concernées dépendent des services fournis au Client, et peuvent inclure, mais ne sont pas limitées à : (i) les prospects, les clients, les partenaires commerciaux et les vendeurs des Clients (qui sont des personnes physiques) ; (ii) les employés ou les personnes de contact des prospects, des clients, des partenaires commerciaux et des vendeurs de l'entreprise du Client ; (iii) les employés, les agents, les conseillers, les collaborateurs indépendants des Clients (qui sont des personnes physiques) ; et (iv) les utilisateurs du Client autorisés par le Client à utiliser les services.

ANNEXE 4 : PROCEDURE DE GESTION DES DEMANDES D'EXERCICE DES DROITS

1. Procédure de gestion d'une plainte ou demande de Personne concernée lorsque le Groupe Talan agit en tant que Sous-traitant



2. Procédure de gestion d'une plainte ou demande de Personne concernée lorsque le Groupe Talan agit en tant que Sous-traitant et que le Responsable de traitement a disparu



Politique de gestion des contrôles des autorités compétentes

Date	Version	Auteur	Modification
13/01/2023	0.1	DPO	Création
14/02/2024	0.2	DPO	Adaptation retours CNIL procédure d'approbation BCR-P (instruction)

Sommaire

• Enjeux et objectifs

La présente politique de gestion des contrôles des autorités compétentes a pour objectif de prévoir les modalités de gestion des demandes des autorités de contrôle compétentes en matière de protection des données personnelles. Le but de cette politique est de s'assurer des conditions de traitement des demandes de contrôle des autorités compétentes pouvant mener des enquêtes et des audits pour s'assurer de la conformité du Groupe Talan aux règles d'entreprise contraignantes (dites *Binding corporate rules* en anglais, « BCR ») adoptées par les entités concernées du Groupe.

L'enjeu principal de cette politique est donc de garantir la conformité du Groupe Talan aux normes et réglementations en vigueur en matière de protection des données personnelles, en minimisant les risques d'infractions et en maintenant une bonne relation avec les autorités compétentes, en fournissant un cadre clair et transparent pour la communication et la coopération lors des contrôles de celles-ci.

• Interactions avec les autorités compétentes en matière de protection des données à caractère personnel

2.1. Procédure de gestion des contrôles des autorités compétentes

2.1.1. Préparation aux contrôles

Le DPO du Groupe Talan s'assure que les personnes clés du Groupe Talan que les autorités compétentes peuvent consulter, ont une compréhension claire de leurs responsabilités en matière de protection des données personnelles et des obligations découlant des BCR du Groupe Talan. Le DPO du Groupe Talan veille à disposer d'une documentation à jour de toutes les procédures, politiques et activités de traitement relatives aux données personnelles au sein du Groupe Talan.

2.1.2. Réception des demandes de contrôle

Lorsqu'un collaborateur du Groupe Talan reçoit une demande d'information ou de contrôle de la part d'une autorité compétente en matière de protection des données personnelles, celui-ci informe le DPO du Groupe Talan, ou le DPO local, identifié au sein de l'entité du Groupe Talan concernée, qui se charge d'informer le DPO Groupe.

2.1.3. Réponse aux demandes de contrôle

Après examen et analyse de la demande de l'autorité compétente, le DPO du Groupe Talan, ou le DPO local si le DPO du Groupe Talan lui délègue la gestion de la demande, répond à la demande de l'autorité compétente dans les délais indiqués par celle-ci, ou à défaut de délai dans un délai raisonnable ne pouvant excéder un (1) mois à compter de la réception de la demande.

Le DPO du Groupe Talan, ou le DPO local en charge de la demande, est la seule personne habilitée à juger de la réponse à transmettre à l'autorité requérante ainsi que de la documentation appropriée à fournir.

2.1.4. Mise en œuvre des actions correctives & Analyse des causes du contrôle

Si à la suite de la réponse, l'autorité compétente émet un avis ou engage une procédure de contrôle avancée, la personne en charge de la gestion met tout en œuvre pour accéder aux demandes de l'autorité compétente. L'autorité compétente est consultée pour déterminer les mesures correctives nécessaires à mettre en œuvre si le traitement des données à caractère personnel doit être poursuivi.

Dans un tel cas, le Groupe Talan met en œuvre toutes les actions correctives nécessaires pour remédier aux problèmes identifiés lors du contrôle et pour garantir la conformité et le respect de la réglementation en matière de protection des données personnelles.

Une fois le contrôle terminé, le DPO du Groupe Talan, ou le DPO local réalise une analyse des causes et facteurs ayant mené au contrôle et s'interroge sur les axes d'amélioration du traitement et de la gestion des données personnelles au sein du Groupe Talan ou de l'entité du Groupe Talan concernée.

2.1.5. Suivi des contrôles

Le DPO du Groupe Talan conserve une documentation détaillée de toutes les interactions avec les autorités compétentes, y compris les réponses fournies et les actions prises en réponse aux constatations des autorités compétentes.

2.2. Les notifications obligatoires aux autorités compétentes

Lorsque cela est exigé par les BCR du Groupe Talan, le RGPD ou toute législation ou réglementation applicables, les entités du Groupe Talan concernées s'engagent à demander les autorisations nécessaires ou à notifier les informations nécessaires aux autorités compétentes.

En particulier, conformément aux engagements formalisés au sein des BCR du Groupe Talan, chaque entité concernée du Groupe Talan s'engage, lorsqu'elle a des raisons de penser que la législation actuelle ou future qui lui est applicable risque de l'empêcher de se conformer aux instructions reçues de la part d'un Responsable du traitement ou de remplir les obligations qui lui incombent en vertu des BCR ou du contrat de service, à en informer sans délai les personnes listées ci-dessous.

- Le DPO du Groupe Talan et le DPO local (s'ils ne sont pas encore informés) ;
- Le Responsable du traitement concerné, qui peut suspendre le transfert des données et/ou résilier le contrat ;
- L'autorité de contrôle dont relève le Responsable du traitement ;
- L'autorité de contrôle dont relève l'entité du Groupe Talan concernée.

• Demande d'une autorité répressive ou d'un organisme étatique de sécurité

L'entité concernée du Groupe Talan agissant en tant qu'importateur de données notifiera rapidement l'exportateur de données si elle :

g) reçoit une demande juridiquement contraignante d'une autorité publique en vertu des lois du pays de destination ou d'un autre pays tiers, en vue de la divulgation de données

à caractère personnel transférées conformément aux BCR ; cette notification comprendra des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse apportée ;

h) prend connaissance de tout accès direct des autorités publiques aux données à caractère personnel transférées en vertu des BCR conformément aux lois du pays de destination ; cette notification comprendra toutes les informations dont dispose l'entité concernée du Groupe Talan agissant en tant qu'importateur de données.

Ces informations doivent également être communiquées au Responsable de traitement et à l'entité responsable du Groupe Talan.

S'il lui est interdit de notifier l'exportateur de données et/ou le contrôleur de données et/ou la personne concernée, l'entité concernée du Groupe Talan agissant en tant qu'importateur de données fera de son mieux pour obtenir une dérogation à cette interdiction, en vue de communiquer autant d'informations que possible et dans les meilleurs délais, et documentera ses meilleurs efforts afin de pouvoir les démontrer à la demande de l'exportateur de données/du Responsable de traitement.
L'entité du Groupe Talan concernée agissant en tant qu'importateur de données fournira à l'exportateur de données / au Responsable de traitement, à intervalles réguliers, autant d'informations pertinentes que possible sur les demandes reçues (en particulier, le nombre de demandes, le type de données demandées, l'autorité ou les autorités requérante(s), si les demandes ont été contestées et le résultat de ces contestations, etc.). Si l'entité concernée du Groupe Talan agissant en tant qu'importateur de données est/ou devient partiellement ou totalement empêchée de fournir à l'exportateur de données / au Responsable de traitement, les informations susmentionnées, elle en informera l'exportateur de données / le Responsable de traitement dans les plus brefs délais.

L'entité concernée du Groupe Talan agissant en tant qu'importateur de données conservera les informations susmentionnées aussi longtemps que les données à caractère personnel seront soumises aux garanties prévues par les BCR, et les mettra à la disposition de l'autorité ou des autorités de contrôle compétente(s) sur demande.

L'entité concernée du Groupe Talan agissant en tant qu'importateur de données examinera la légalité de la demande de divulgation, en particulier si elle reste dans les limites des pouvoirs accordés à l'autorité publique requérante, et contestera la demande si, après une évaluation minutieuse, elle conclut qu'il y a des motifs raisonnables de considérer que la demande est illégale en vertu des lois du pays de destination, des obligations applicables en vertu du droit international et des règles de la courtoisie internationale.

L'entité concernée du Groupe Talan agissant en tant qu'importateur de données poursuivra, dans les mêmes conditions, les possibilités d'appel. Lorsqu'elle conteste une demande, l'entité concernée du Groupe Talan agissant en tant qu'importateur de données demandera des mesures provisoires en vue de suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente ait statué sur son bien-fondé. Elle ne divulguera pas les données à caractère personnel demandées tant qu'elle n'y sera pas contrainte par les règles de procédure applicables.

L'entité concernée du Groupe Talan agissant en tant qu'importateur de données documentera son évaluation juridique et toute contestation de la demande de divulgation et, dans la mesure où les lois du pays de destination l'autorisent, mettra la documentation à la disposition de l'exportateur de

données / du Responsable de traitement. Elle la mettra également à la disposition de la ou des autorité(s) de contrôle sur demande.

L'entité concernée du Groupe Talan agissant en tant qu'importateur de données fournira le minimum d'informations autorisé lorsqu'elle répondra à une demande de divulgation, sur la base d'une interprétation raisonnable de la demande.

En tout état de cause, les transferts de données à caractère personnel par une entité du Groupe Talan à une autorité publique, quelle qu'elle soit, ne sauraient être massifs, disproportionnés et sans distinction, ni aller au-delà de ce qui est nécessaire dans une société démocratique.