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

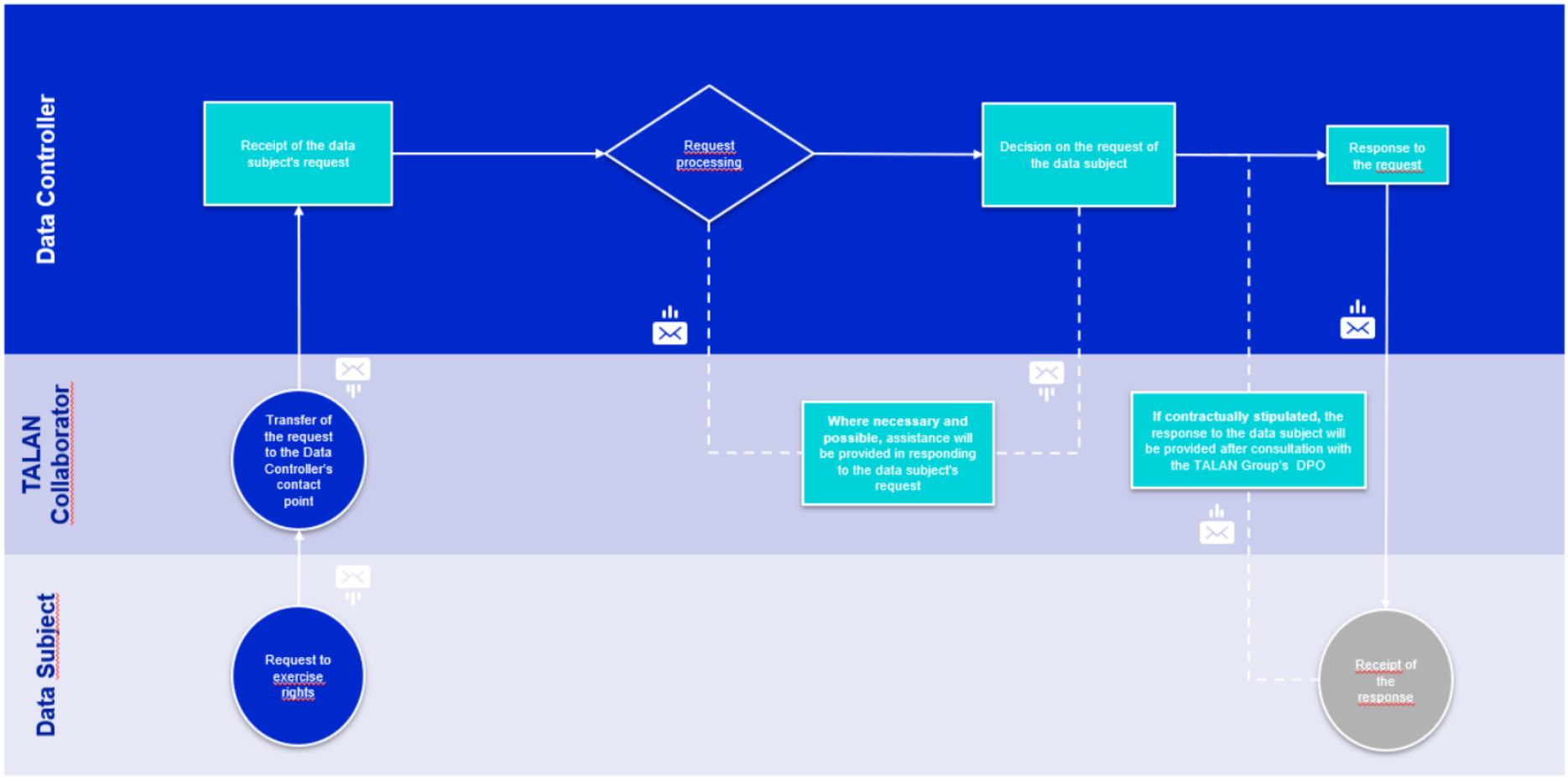
						700-60 rue Saint Jacques Montreal, Quebec, H2Y1L5, CANADA
		USA	1	Talan LLC	IT services and technical assistance	Limited liability company registered under the laws of the State of Delaware with the Delaware Trade and Companies Register under the identification number 20-4193242 33 Irving Place - New 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

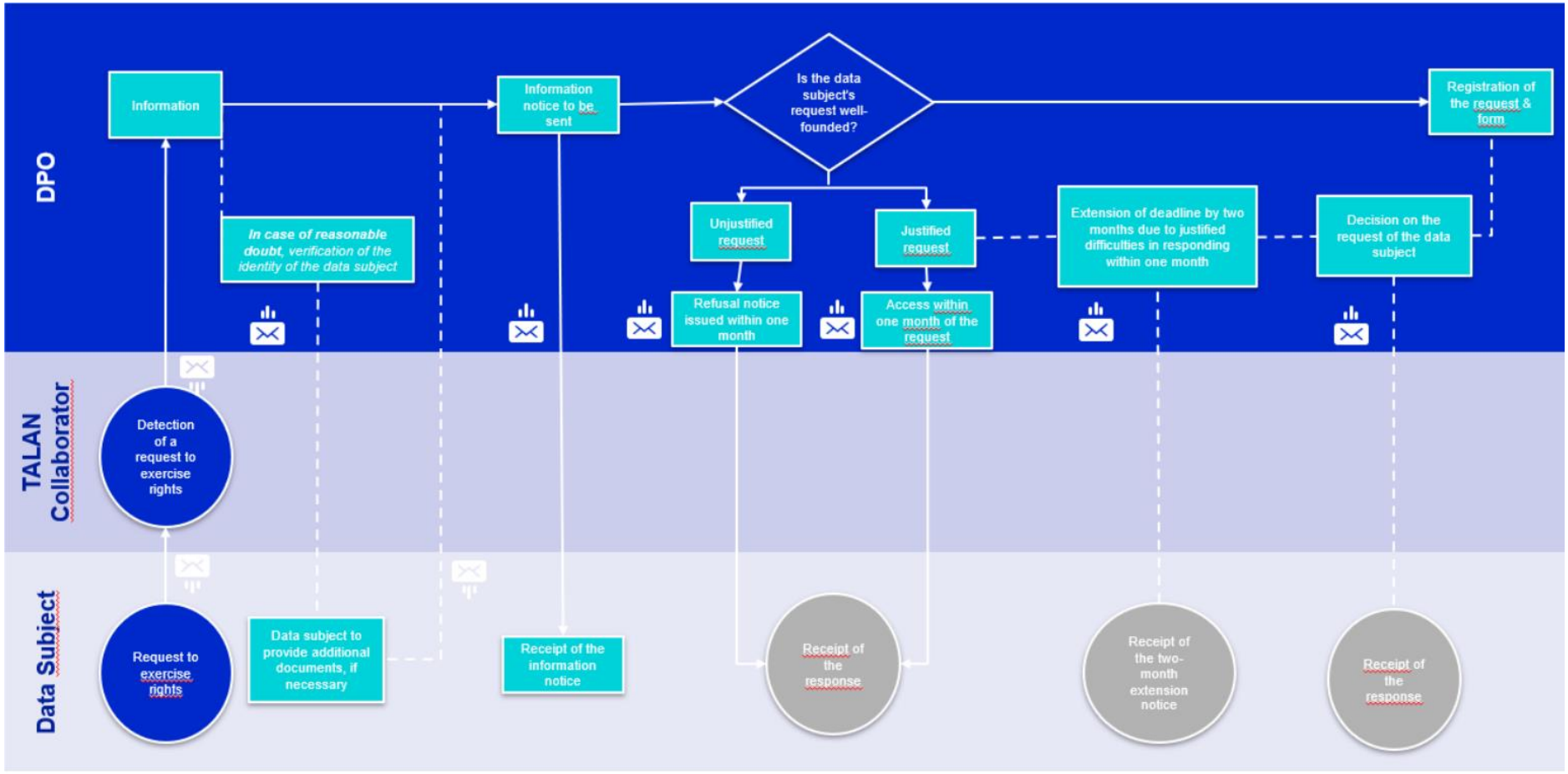
Purposes of data transfer and further processing	TALAN processes the personal data of its Clients in order to carry out their projects related to IT services, management consulting, software creation and publishing, technical assistance, etc. The purpose of transferring the Client's personal data is 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.