ARDIAN

# BINDING CORPORATE RULES - SUMMARY

## Intra group data transfers

**May 2024**

# TABLE OF CONTENT

# 1. PREAMBLE

The aim of this document is to provide a concise and easy to understand synthesis of Ardian's Binding Corporate Rules. The purpose of these Binding Corporate Rules is to facilitate and organize the secure transfer of personal data across borders between entities of the Ardian group in compliance with applicable data protection laws.

# 2. DEFINITIONS

The terms below will have the following meaning:

- "adequacy decision": implementing act taken by the European Commission which determines a third country as ensuring an adequate level of protection of personal data according to the European Union Data Protection regulation 2016/679;
- "competent data protection authority": the European Economic Area data protection authority competent for the data exporter;
- "controller": the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- "consent" of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- "data exporters": endorsing entities established in France and other locations in the European Economic Area (including entities established in countries benefiting from an adequacy decision) having endorsed these Binding Corporate Rules and transferring personal data to another endorsing entity established in a country outside the European Economic Area (excluding entities established in countries benefiting from an adequacy decision) not ensuring an adequate level of protection;
- "data importers": endorsing entities established in a country outside the European Economic Area not ensuring an adequate level of protection according to the European Union Data Protection regulation 2016/679, and receiving from the data exporter elements intended to be processed in accordance with these Binding Corporate Rules;
- "data subject": an individual to whom the data covered by the processing relates, whether or not citizen or resident of an European Economic Area country;
- "endorsing entity": entities having singed these Binding Corporate Rules, namely ARDIAN France, its sister companies and their establishments, its subsidiaries and their establishments as well as any other company in which the aforementioned companies have a share of the registered capital regardless the amount of such share;
- "personal data" or "data": any information relating to a natural person ("data subject") who is or 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. In order to determine whether a person is identifiable, all the means that the controller or any other person uses or may have access to should be taken into consideration;
- "personal data breach": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- "processor": a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- “processing of personal data” or “processing”: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- “profiling”: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

- “recipient”: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

- “third parties”: the natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

- “transfer”: communicating, copying or moving personal data via a network, or communicating, copying or moving these data from one media to another, whatever the type of media, to the extent that the data are subject to processing in the recipient country.

# 3. ENDORSEMENT

The data exporters and the data importers (i.e. Ardian endorsing parties) agree to comply with these Binding Corporate Rules throughout the term of their endorsement, subject to compliance with local regulations.

# 4. ENTITY WITH DELEGATED DATA PROTECTION RESPONSIBILITIES

ARDIAN France shall be the entity with data protection responsibilities. As the entity with delegated data protection responsibilities, it will be:

- in charge of ensuring the proper implementation of these Binding Corporate Rules;
- the prime contact with the supervisory authorities and data subjects; and
- responsible for any violation of the Binding Corporate Rules by an endorsing entity.

# 5. DESCRIPTION OF THE PROCESSING

The categories of the data, the type of processing and their purposes, the categories of data subjects and the scope of the transfers within the endorsing entities are detailed for each processing in Appendix 3. These Binding Corporate Rules apply to all personal data transferred to endorsing entities outside the European Economic Area and onwards transfers to other endorsing entities outside the European Economic Area, as detailed in the appendices hereto. The list of endorsing entities and contact details of the Ardian group are provided in Appendix 2.

Ardian Privacy Officer and additional privacy functions, as described in Appendix 1, carry out regular verifications of the processing operations carried out in the context of these Binding Corporate Rules, in particular in relation to the categories of personal data processed and countries where are located data importers. The entity with delegated data protection responsibilities and, where applicable, the endorsing entities ensure that the Privacy Officer and additional privacy functions have access to the necessary information and tools to conduct this verification.

# 6. UNDERTAKING GIVEN BY DATA EXPORTER

## 6.1. Quality of the data collected

The data exporters undertake that the personal data transferred are:

- obtained and processed fairly, lawfully and in a transparent manner in relation to the data subject;
- obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are obtained and their further processing;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- stored in a format that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, as set out in article 12 “Security of processing and data”;
- only onward transferred outside the European Economic Area in accordance with article 13 “Restrictions on onward transfers”.

## 6.2. Purpose limitation

Data exporters warrant that:

- the transfer of the personal data is carried out for a specified, explicit and legitimate purpose; and
- the data transferred is not processed in a manner that is incompatible with the purpose of the transfer.

## 6.3. Lawfulness of the processing

Data exporters shall only process personal data if:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject, as laid down by European Union law or applicable Member State law;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, as laid down by European Union law or applicable Member State law;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

## 6.4. Special categories of data and criminal offences data

Data exporters shall not collect or process personal data that reveals, directly or indirectly, the racial and ethnic origins, the political opinions, philosophical or religious beliefs or trade union affiliation of persons, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data which concern their sexual life or sexual orientation, except if:

- data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where European Union or Member State law provide that the prohibition on the processing of special categories of data may not be lifted by the data subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by European Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of European Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or Member State law or pursuant to contract with a health professional and subject to those data being processed by or under the responsibility of a professional subject to the obligation of professional secrecy under European Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under European Union or Member State law or rules established by national competent bodies;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of European Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on European Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Data exporters shall not collect or process personal data relating to criminal convictions and offences or related security measures, except if the processing is carried out under the control of official authority or when the processing is authorised by European Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

## 6.5. Data storage limit

Each endorsing entity shall store the personal data in accordance with applicable laws and regulations as applicable to the endorsing entity, and for a period no longer than is necessary for the purposes for which they are obtained and processed.

# 7. UNDERTAKING GIVEN BY DATA IMPORTER

## 7.1. General undertakings

Data importers, whether acting as controller or processor, may only process and/or transfer personal data to another importer in compliance with the conditions set out in article 6 “Undertakings given by data exporter”. More generally, data importers shall comply with all obligations set forth in article 6 “Undertakings given by data exporter”, where applicable.

## 7.2. Government access requests

Without prejudice to the obligation of the endorsing entity acting as data importer to inform the data exporter of its inability to comply with the commitments contained in the Binding Corporate Rules (as set forth in article 11):

- The endorsing entity acting as data importer will promptly notify the data exporter and, where possible, the data subject (if necessary with the help of the data exporter) if it:
  - 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 Binding Corporate Rules; such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided;
  - becomes aware of any direct access by public authorities to personal data transferred pursuant to the Binding Corporate Rules in accordance with the laws of the country of destination; such notification will include all information available to the data importer.
- If prohibited from notifying the data exporter and / or the data subject, the 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.
- The data importer will provide the endorsing entity acting as data exporter, 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 data importer is or becomes partially or completely prohibited from providing the data exporter with the aforementioned information, it will, without undue delay, inform the data exporter accordingly.
- The data importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by the Binding Corporate Rules, and shall make it available to the competent data protection authorities upon request.
- The 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 data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the 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 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. It will also make it available to the competent data protection authorities upon request.

- The 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.

Transfers of personal data by an endorsing 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.

# 8. RIGHTS OF DATA SUBJECTS

## 8.1. General rights

In the event that personal data is transferred to an endorsing entity established in a country outside the European Economic Area (excluding entities established in countries benefiting from an adequacy decision) that does not ensure an adequate level of protection, any data subject may enforce and is entitled to:

- obtain a copy of these Binding Corporate Rules, or be provided at least with the following information, in full, which shall be up-to-date, and presented in a clear, intelligent and transparent way:

  - a description of the scope of the Binding Corporate Rules (as set out in article 5 “Description of the processing”);
  - a copy of the clauses relating to liability (as set out in article 17 “Liability” and article 21 “Jurisdiction”), to the data protection principles (as set out in article 6 “Undertakings given by data exporter” and article 7 “Undertaking given by data importer”), to the lawfulness of the processing (as set out in article 6 “Undertakings given by data exporter” and article 7 “Undertaking given by data importer”), to security and personal data breach (as set out in article 12 “Security of processing and data”), to restrictions on onward transfers (as set out in article 13 “Restrictions on onward transfers”), to the rights of the data subjects (as set out in article 8 “Rights of data subjects”); and
  - the list of definitions used in these clauses (as set out in article 2 “Definitions”).

  Data subjects may obtain such copy or information using the services referred to in Appendix 1 “Contact”; in a reasonable time on a simple request.

  These Binding Corporate Rules are published on the intranet of the endorsing entities. In addition, a summary of the Binding Corporate Rules, including all the required information listed above, is made available to all data subjects on the public website of the entity with delegated data protection responsibilities;

- be informed of any update of these Binding Corporate Rules and of the list of endorsing entities, if any, (i) as published within a reasonable time on the intranet and/or website of the endorsing entities; as well as (ii) upon request, using the services referred to in Appendix 1 “Contact”, in a reasonable time;

- be informed of the transfer of the personal data relating to them, the purpose of the transfer, the recipient or the categories of recipients, the place where the data recipient is established and the existence of adequate protection or appropriate safeguards;

- obtain information on their rights, as set forth in this article 8 “Rights of data subjects”, with regard to the processing of their personal data, and on the means to exercise those rights;

- obtain information on the processing of their personal data, the disclosure of all data processed relating to them and as appropriate, the rectification, erasure or restriction, and, as applicable, the notification regarding rectification, erasure or restriction of the personal data processed, as further described in article 8 below;

- object to the processing of the personal data relating to them on compelling legitimate grounds relating to their particular situation, as further described in article 8.7 below;

- request not to be subject to decisions based solely on automated processing including profiling, as further described in article 8.8 below;

- claim enforcement of:
  - the endorsing entities' duty to cooperate with each other and/or with the competent data protection authorities such as set out in article 14 "Co-operation" hereof, regarding compliance with the obligations set forth in this article 8 "Rights of data subjects";
  - the obligation for the endorsing entities to immediately inform the entity with delegated data protection responsibilities if the legislation applicable to it may prevent it from fulfilling its obligations under these Binding Corporate Rules, in accordance with article 11 "National mandatory requirements for entities" hereof;
  - the obligations applicable in case of government access requests, as set out in article 7.2;
  - the obligation to comply with applicable data protection principles, in particular the lawfulness of processing, as set out in article 6 "Undertakings given by data exporter";
  - the obligation not to make onward transfer outside the group without complying with the conditions set forth in article 13 "Restrictions on onward transfers" hereof;
  - the security and confidentiality obligation, including with respect to personal data breach, such as set out in article 12 "Security of processing and data" hereof.

- any applicable judicial remedy in case of breach of this article 8 "Rights of data subjects" and the right to be represented before competent courts by a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data, as set out in article 21 "Jurisdiction";

- obtain, when they have suffered damage as a result of a breach of this article 8 "Rights of data subjects":
  - redress of the actions or inactions that violated the Binding Corporate Rules; and
  - if appropriate, compensation for damage suffered, as set out in article 20 "Liability".

- contact the complaint-handling service, in accordance with article 16 "Complaint Handling" hereof, for any violation of their rights stated herein;

- apply to a data protection authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement, for any violation of their rights stated herein;

- refer the matter to the competent courts, in accordance with article 21 "Jurisdiction" hereof, for any violation of their rights stated herein.

## 8.2. Right of information

**TRANSPARENCY**

The endorsing entities, acting as controller, shall take appropriate measures to provide any information referred to in this article 8.2 and any communication under articles 8.3 to 8.8 and 12.1 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The information shall be provided to data subject free of charge. Where requests from a data subject

are manifestly unfounded or excessive, in particular because of their repetitive character, the endorsing entity may either: (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The endorsing entity shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

The endorsing entities shall facilitate the exercise of data subject rights under articles 8.3 to 8.8 below and provide information to the data subject on action taken on a request with those rights, in accordance with article 16 “Complaint handling”.

**INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE COLLECTED FROM THE DATA SUBJECT**

Where personal data relating to a data subject are collected from the data subject, and unless the data subject already has the information, the endorsing entity acting as controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on legitimate interests, the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on data subjects’ consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a competent data protection authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
- where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as listed above.

**INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE NOT COLLECTED FROM THE DATA SUBJECT**

Where personal data have not been obtained from the data subject, the endorsing entity acting as controller shall provide the data subject with the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;

- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on legitimate interests, the legitimate interests pursued by the controller or by a third party;
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on data subjects' consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a competent data protection authority;
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
- where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as listed above.

The endorsing entity acting as controller shall provide the information listed above: (i) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (ii) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (iii) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

The endorsing entity acting as controller may not provide the information listed above if:

- the data subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort, or in so far as the provision of this information is likely to render impossible or seriously impair the achievement of the objectives of that processing, in which cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure is expressly laid down by European Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by European Union or Member State law, including a statutory obligation of secrecy.

## 8.3. Right of access

Unless it adversely affects the rights and freedoms of others, the data subject shall have the right to obtain from endorsing entity acting as controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data

and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a competent data protection authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

The endorsing entity acting as controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the endorsing entity may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

## 8.4. Right to rectification

The data subject shall have the right to obtain from the endorsing entity acting as controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The endorsing entity acting as controller shall communicate any rectification of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The endorsing entity shall inform the data subject about those recipients if the data subject requests it.

## 8.5. Right to erasure

The data subject shall have the right to obtain from the endorsing entity acting as controller the erasure of personal data concerning him or her without undue delay and the endorsing entity shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to article 8.7 and, where applicable there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in the European Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services.

Where the endorsing entity acting as controller has made the personal data public and is obliged

pursuant to the above to erase the personal data, the endorsing entity, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The data subjects' right to erasure shall not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by European Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

The endorsing entity acting as controller shall communicate any erasure of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The endorsing entity shall inform the data subject about those recipients if the data subject requests it.

## 8.6. Right to restriction of processing

The data subject shall have the right to obtain from the endorsing entity acting as controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to article 8.7 pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted in accordance with the above, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State.

A data subject who has obtained restriction of processing pursuant to the above shall be informed by the endorsing entity acting as controller before the restriction of processing is lifted.

The endorsing entity acting as controller shall communicate any restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The endorsing entity shall inform the data subject about those recipients if the data subject requests it.

## 8.7. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is (i) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the endorsing entity acting as controller or (ii) necessary for the purposes of the legitimate interests pursued by the endorsing entity acting as controller or by a third party, including profiling based on those legal bases. The endorsing entity acting as controller shall no longer process the personal data unless the endorsing entity demonstrates compelling legitimate grounds for the processing which

override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the right referred to above shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

## 8.8. Automated individual decision-making

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The above shall not apply if the decision is:

- authorised by European Union or Member State law to which the endorsing entity acting as controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;
- (i) necessary for entering into, or performance of, a contract between the data subject and a controller; or (ii) based on the data subject's explicit consent. In such cases, the endorsing entity acting as controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the endorsing entity, to express his or her point of view and to contest the decision.

The above exceptions shall not apply if the processing is based on special categories of data, unless the processing is based on the data subject’s consent or is necessary for reasons of substantial public interest, on the basis of European Union or Member State law.

# 9. GUARANTEE OF IMPLEMENTATION

The endorsing entities agree to take such measure as may be necessary to ensure that each of them will adjust its processing activities to meet the requirements of these Binding Corporate Rules, subject to their compliance with local rules.

In the event these Binding Corporate Rules are not complied with, and subject to their compliance with local rules, any data subject may have recourse to the complaint process, the competent data protection authority and/or the competent courts.

# 10. TRAINING AND EDUCATION

The endorsing entities agree to implement up-to-date training programs dedicated to the protection of personal data and these Binding Corporate Rules for their employees that have permanent or regular access to personal data, that are involved in the collection of personal data or in the development of tools used to process personal data. These training programs shall notably cover procedure of managing requests for access to personal data by public authorities, and be provided to the abovementioned employees at least once (1) a year

Employees are informed of the disciplinary sanctions that may be taken in the event that they fail to comply with these rules.

# 11. NATIONAL MANDATORY REQUIREMENTS FOR ENTITIES

The data exporters will use the Binding Corporate Rules as a tool for transfers only where they have assessed (and documented such assessment and supplementary measures) that the law and practices in the third country of destination applicable to the processing of the personal data by the endorsing 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 Binding Corporate Rules. This is based on the understanding that laws and practices are not in contradiction with the Binding Corporate Rules where they respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society. Developments in the third countries to which data is transferred to shall be monitored in case it affects the initial assessment.

The data importer will promptly notify the data exporter if 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 the Binding Corporate Rules. Upon such notification, the data exporter shall identify supplementary measures to be adopted.

If the Binding Corporate Rules cannot be complied, the transfer shall be suspended until compliance is again ensured or the transfer is ended. Upon termination of the transfer, personal data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the endorsing entity acting as data exporter, be returned to it or destroyed in their entirety.

# 12. SECURITY OF PROCESSING AND DATA

## 12.1. Security obligations

The endorsing entities agree to take all useful precautions, with regard to 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, to preserve the security of the data transmitted, stored or otherwise processed and, in particular, prevent their accidental or unlawful loss, alteration or destruction, and any unauthorized or unlawful processing or disclosure. The endorsing entities in particular agree to take appropriate technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. This notably includes the following measures:

- internal policies in relation to the security of the Ardian's information system (e.g., information security policy) and on the protection of personal data (e.g., data breach policy);
- asset management measures (e.g., asset management policy);
- access control measures (e.g., access control policy, user access right management policy, privileged access management, authentication system, password management system);
- cryptography (e.g., cryptography and key management policy);
- physical and environmental security measures (e.g., environmental and physical security, entry controls, clear desk and clear screen policy);
- operations security measures (e.g., change and capacity management, separation of environments, controls against malware, information backup & restore, event logging, management of technical vulnerabilities);
- communications security measures (e.g., network security management, non-disclosure agreements, encryption in transit and at rest);
- system acquisition, development and maintenance measures (e.g., secure development policy, system security testing, system acceptance testing);
- supplier relationships security measures (e.g., Third-party relationship management);
- risk and control management (e.g., control plan, risk management process);
- information security incident management (e.g., information security incident and exception procedure, threat intelligence policy);
- business continuity management (e.g., business continuity plan, business impact analysis).

In the event that personal data is transferred to processors, each processor shall offer adequate guarantees to ensure the implementation of the security and confidentiality measures.

## 12.2. Notification of personal data breaches

The endorsing entities shall notify, without undue delay, any personal data breaches to the entity with delegated data protection responsibilities and to the Privacy Officer and/or relevant contacts, as listed in appendix 1, as well as to the endorsing entity acting as a controller when an endorsing entity acting as a processor becomes aware of a personal data breach.

The endorsing entities shall notify, without undue delay, and, where feasible, not later than seventy-two (72) hours after having become aware of the personal data breach to the competent data protection authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The endorsing entities shall notify, without undue delay to data subjects, where the personal data breach is likely to result in a high risk to their rights and freedoms or where the competent data protection authority requires data subjects to be notified. This notification shall describe in clear and plain language the nature of the personal data breach and contain at least (i) the name and contact details of the data protection officer or other contact point where more information can be obtained; (ii) a description of the likely consequences of the personal data breach; and (iii) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

This notification to data subjects shall not be required if:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to above is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or
- the competent data protection authority decides that any of the above conditions are met.

The endorsing entities shall document any personal data breach (comprising the facts relating to the personal data breach, its effects, and the remedial action taken), and such documentation should be made available to the competent data protection authority upon request.

# 13. RESTRICTION ON ONWARD TRANSFERS

In the event that personal data is transferred from the endorsing entities to non-endorsing entities outside the European Economic Area, the entities at the origin of the transfers agree to inform the data subjects in accordance with article 8.2.

These onward transfers may only be carried out if one of the following conditions for transfers applies in order to ensure that the level of protection of natural persons guaranteed by these Binding Corporate Rules is not undermined:

- The non-endorsing entity is located in a country benefiting from an adequacy decision, i.e., a decision from the European Union Commission which decided that this country ensures an adequate level of protection of personal data;
- In the absence of an adequacy decision, the non-endorsing entity has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. These appropriate safeguards may be provided for by:

- a legally binding and enforceable instrument between public authorities or bodies;
- standard data protection clauses adopted by the European Union Commission;
- standard data protection clauses adopted by a competent data protection authority and approved by the European Union Commission;
- an approved code of conduct, together with binding and enforceable commitments of the controller or processor in the country of the non-endorsing entity to apply the appropriate safeguards, including as regards data subjects' rights;
- an approved certification mechanism, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- subject to the authorization from a competent data protection authority, (i) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country; or (ii) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

> In the absence of an adequacy decision or appropriate safeguards, one of the following conditions applies:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
- the transfer is made from a register which according to European Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by European Union or Member State law for consultation are fulfilled in the particular case.

For all of these onward transfers, each endorsing entity shall conclude a contract with the non-endorsing entities:

> when the transfer is made within the European Union or a country ensuring an adequate level of protection (including entities established in countries benefiting from an adequacy decision), such contract shall include a clause specifying the security and confidentiality measures taken by the entity to which the transfer is made; the clause shall remind that said entity can in any case act only on instructions from the endorsing entity;

> when the transfer is made to a non-endorsing entity established outside the European Union (excluding entities established in countries benefiting from an adequacy decision), and does not benefit from an exception authorizing the transfer, such contract shall be drafted on the basis of standard contractual clauses adopted by the European Commission.

Special reference will be made to the standard contractual clauses described above during the regular audits conducted on the application of these Binding Corporate Rules.

# 14. CO-OPERATION

The endorsing entities agree to co-operate and help each other to handle a request or complaint from data subjects, closely co-operate with the competent personal data protection authorities and follow the audit requirements.

The endorsing entities agree to abide by the advice and recommendations of the competent data protection authorities in the place where they are established.

# 15. CONTROL OF COMPLIANCE

The endorsing companies agree to appoint one or more officers in charge of ensuring compliance with these Binding Corporate Rules. These contacts include the Privacy Officer and additional privacy functions such as local compliance officers, as detailed in Appendix 1. The contacts are in charge of, among other tasks, reporting on compliance to the highest management level.

The entity with delegated data protection authorities and, where applicable, the endorsing entities ensure that these contacts have the necessary resources to carry out their tasks (including time required, access to financial and documentary resources, collaborators if necessary or external support).

In addition, the application of the principles laid down in these Binding Corporate Rules is guaranteed by the realization of audits carried out on a regular basis, and at least once (1) a year.

The individuals deciding or conducting the audit program shall be guaranteed independence as to the performance of their duties related to these audits. The audit program covers all aspects of the Binding Corporate Rules

# 16. COMPLAINT HANDLING

Data subjects may lodge a complaint about unlawful processing or an act relating to them that is incompatible with these Binding Corporate Rules, by sending a letter or e-mail to dataprivacyofficer@ardian.com or by writing to Ardian, Data Protection, 20 Place Vendome, 75001 Paris, to which should be attached a copy of an identity document. The letter (or e-mail) must be sent with a document proving the identity of the data subject and must describe the reasons of the complaint and include any relevant supporting document.

The data subject is informed that he or she may in any case apply to a data protection authority or to a competent court in accordance with article 21 “Jurisdiction” hereof, such right being independent on the data subject having used the complaint handling process detailed above beforehand.

The person responsible for investigation:

- manages and receives complaints lodged by data subjects;
- helps to find a solution;
- where applicable, opens an investigation to gather and review the facts;
- shall act with independence, neutrality and impartiality in the exercise of their mission.

Upon receipt of the complaint, and no later than within five (5) business days, the data subject receives information on the identity of the employee in charge of handling the complaint and the approximate length of time required to handle the complaint, or an immediate answer or a request for additional documents.

The data subject is informed on actions taken in relation to the complaint without undue delay, and in any event within one (1) month. The data subject is kept regularly informed of the progress of the review of the complaint.

In order to ensure that the above delay is complied with, the period to review a complaint may not exceed one (1) month from the receipt by the designated individual of the entity concerned of the request (letter or e-mail) of the data subject who has given proof of his or her identity, including where the request is subsequently submitted to the Privacy Officer of the entity with delegated data protection responsibilities. Taking into account the complexity and number of the requests, that one-month period may be extended at maximum by two (2) further months, in which case the complainant should be informed accordingly.

At the end of the review, after legal analysis, a letter is sent to the data subject informing them (i) whether the complaint is found justified, in which case the data subject will be informed of the actions taken as a result, (ii) whether the complaint is dismissed, in which case the data subject will be informed of the reasons for dismissal, (iii) and in all cases, of the other available remedies (the competent data protection authorities or the competent courts in accordance with article 21 “Jurisdiction”, and where applicable the Privacy Officer if the data subject has not already referred the matter to them).

# 17. LIABILITY

The entity with delegated data protection responsibilities accepts responsibility for and agrees to take, at any given time, the necessary action to remedy the acts of endorsing entities established outside the European Economic Area and not ensuring a sufficient level of protection and to pay compensation for any damages (whether material or non-material) resulting from the violation of the Binding Corporate Rules by said entities.

Where data subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of these Binding Corporate Rules, it will be for the entity with delegated data protection responsibilities (i.e. Ardian France) to prove that the endorsing entity outside of the European Economic Area was not responsible for the breach of the Binding Corporate Rules giving rise to those damages, or that no such breach took place. If the entity with delegated data protection responsibilities can prove that the endorsing entity established outside the European Economic Area and not ensuring a sufficient level of protection is not liable for the act resulting in the damage claimed by the data subject, Ardian France will discharge itself from any responsibility.

The endorsing entities may be partially or totally exempted from liability as the controller if they establish that they are not responsible for the violation or the damage.

Ardian France has sufficient assets to cover the payment of compensation for breaches of these Binding Corporate Rules.

# 18. SANCTIONS

Sanctions may be taken in the event of (i) breach of the Binding Corporate Rules, (ii) non-compliance with audit recommendations, and (iii) failure to cooperate with data protection authorities.

Sanctions may consist of disciplinary measures taken against the employees who breach the law or the Binding Corporate Rules. These sanctions may be accompanied by other measures, if ordered by the competent independent administrative or judicial local authorities.

# 19. UPDATES

## 19.1. Updates to the content of the Binding Corporate Rules

In the event of changes to the content of these Binding Corporate Rules, the text shall be reported to the relevant data protection authority and without undue delay to the endorsing entities.

Where a modification to the Binding Corporate Rules would possibly be detrimental to the level of the protection offered by the Binding Corporate Rules or significantly affect them, it must be communicated in advance to the data protection authorities with a brief explanation of the reasons for the update. In this case, the data protection authorities will also assess whether the changes made require a new approval.

Any updates to the list of entities or any substantial changes to the Binding Corporate Rules should

be reported once a year to the data protection authorities with a brief explanation of the reasons for the changes. The data protection authorities should also be notified once a year (i) in instances where no changes have been made, and (ii) of the confirmation regarding assets.

Any change to the Binding Corporate Rules shall be reflected, without undue delay, in this summary.

## 19.2. Updates to the list of the endorsing entities

Any changes to the list of the entities should be reported once a year to the relevant data protection authorities.

No transfer is made to a new entity until the new entity is effectively bound by these Binding Corporate Rules and can deliver compliance.

Any change to the list of endorsing entities shall be reflected, without undue delay, in this summary.

# 20. GOVERNING LAW

These Binding Corporate Rules shall be governed by the law of the country in which the data exporter is established, subject to their compliance with local regulations.

# 21. JURISDICTION

The data subject may apply to (i) a data protection authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement, and/or (ii) the competent court in order to obtain compensation for the damage suffered as a result of a violation of the foregoing provisions.

The competent courts shall be:

- the court of the place in which the data exporter is established within the European Union (or the country benefiting from an adequacy decision if established in such country); or
- the court of the place in which the entity with delegated data protection responsibilities is established; or
- with respect to data subjects, the court of the place where the data subject has their habitual residence within the European Union.

In any case, if an endorsing entity outside the European Economic Area violates these Binding Corporate Rules, the courts or other judicial authorities in the European Economic Area will have jurisdiction, and data subjects will have the rights and remedies against the entity with delegated data protection responsibilities as if the violation had been caused by the latter in the Member State in which it is based.

Any dispute related to the competent data protection authorities' exercise of supervision of compliance with these Binding Corporate Rules will be resolved by the courts of the Member State of the competent data protection authority concerned, in accordance with that Member State's procedural law, and the endorsing entities agree to submit themselves to the jurisdiction of these courts.

# 22. EFFECTIVE DATE/TERM

These Binding Corporate Rules will be effective for an unlimited period of time upon the date of the first signature by the endorsing entities.

An endorsing entity acting as data importer, which ceases to be bound by the Binding Corporate Rules may keep, return, or delete the personal data received under the Binding Corporate Rules. If the data exporter and data importer agree that the data may be kept by the data importer, protection must be maintained in accordance with an adequacy decision or appropriate safeguards.

# 23. LIST OF APPENDIXES

- APPENDIX 1 – CONTACT
- APPENDIX 2 – LIST OF ENDORSING ENTITIES
- APPENDIX 3 – MATERIAL SCOPE OF THE BCR

# APPENDIX 1 - CONTACT

To facilitate the exercise of privacy rights under applicable data protection law, individuals may contact the designated team members responsible for data protection and privacy matters. These contacts include the Data Protection Officer (DPO), Privacy Champions, and the Chairs of the Privacy Committee, each with specialized expertise in Privacy Law, Compliance, IT, and specific regions or countries.

For privacy and security reasons, we do not publicly list the personal contact details, such as direct email addresses, phone numbers, or photos, of the individuals in these roles. Instead, individuals wishing to exercise their rights or seek assistance with privacy-related matters can reach out via the following contact points:

- **Email**: dataprivacy@ardian.com
  Emails sent to this distribution list are monitored by the Data Protection Officer, Privacy Champions, and the Chairs of the Privacy Committee. Depending on the nature of the request, the appropriate individual or team will respond to the inquiry.
- **Postal Address**: Ardian, Data Protection Officer, 20 Place Vendôme, 75001 Paris, France

When reaching out, please specify your region or country, and the request will be directed to the DPO and the relevant Privacy Champion for further handling.

This ensures that all inquiries are appropriately managed while protecting the privacy of our team members.

# APPENDIX 2 - LIST OF ENDORSING ENTITIES

**ARDIAN HOLDING SAS**

20 PLACE VENDOME,
75001 PARIS

FRANCE

TEL: (+33) 1 47 71 92 00

**ARDIAN FRANCE SA**

20 PLACE VENDOME,
75001 PARIS

FRANCE

TEL: (+33) 1 41 71 92 00

**ARDIAN INVESTMENT UK LTD**

1 GRAFTON STREET
LONDON, W1S 4FE

UNITED KINGDON

TEL: (+44) 207 154 43 00

**ARDIAN GERMANY GMBH**

AN DER WELLE 4,
D-60322 FRANKFURT

GERMANY

TEL: (+49) 69 50 50 41 500

**ARDIAN GERMANY INVESTMENT OPPORTUNITES GmbH**

AN DER WELLE 4,
D-60322 FRANKFURT

GERMANY

TEL: (+49) 69 50 50 41 500

**ARDIAN INVESTMENT SWITZERLAND AG**

BAHNHOFSTRASSE 20 -
8001 ZURICH

SWITZERLAND

TEL: (+41) 44 213 27 27

**ARDIAN INVESTMENT SWITZERLAND HOLDING AG**

BAHNHOFSTRASSE 20 -
8001 ZURICH

SWITZERLAND

TEL: (+41) 44 213 27 27

**ARDIAN ITALY S.R.L**

GALLERIA DE CRISTOFORIS,
20122 MILAN

ITALY

TEL: (+39) 02 584 42 401

**ARDIAN INVESTMENT SINGAPORE PTE LTD**

1 TEMASEK AVENUE
#20-02A MILLENIA

TOWER, SINGAPOUR 039192

TEL: (+65) 65 13 34 10

**ARDIAN US LLC**

1370 AVENUE OF THE AMERICAS,
NEW YORK, NY 10019-4602

UNITED STATES OF AMERICA

TEL: (+1) 212 6418604

**ARDIAN JERSEY LIMITED**

THIRD FLOOR - 27 ESPLANADE
ST HELIER, JERSEY

JE2 3QA

TEL: (+44) 1534 601200

**ARDIAN LUXEMBOURG S.A R.L.**

24, AVENUE EMILE REUTER

L-2420 LUXEMBOURG

TEL: (+352) 27 44 48 1

**ARDIAN BEIJING CONSULTING COMPANY LIMITED**

UNIT 20-22, LEVEL 47, CHINA WORLD
TOWER, NO. 1 JIAN GUO MEN WAI
AVENUE, BEIJING 100004,

CHINA

TEL: (+86)10 6580 9000

**ARDIAN JAPAN CO. LTD.**

TEL: (+81) 3 5220 0010

MARUNOUCHI NIJUBASHI BUILDING 21F,
23-2-3 MARUNOUCHI,
CHIYODA-KU,
TOKYO 100-0005,

JAPAN

**ARDIAN KOREA**

TEL: (+82) 2 6030 8750

27F, WEST CENTER
CENTER 1 BUILDING 26 EUUIRO 5-GIL,
JUNG-GU, SEOUL 04539

SOUTH KOREA

**ARDIAN CHILE SPA**

TEL: (+562) 32784600

AV. APOQUINDO 2929,
OFICINA 1800, PISO 18
SANTIAGO, LAS CONDES

CHILE

**ARDIAN SPAIN S.L.**

TEL: (+34) 913 108 400

CALLE FORTUNY 6, PLANTA 5
28010 MADRID

SPAIN

**ARDIAN LIMITED**

TEL: (+971) 50 316 22 14

AL KHATEM TOWER - FLOOR 23
ABU DHABI GLOBAL MARKET SQUARE
AL MARYAH ISLAND, ABU DHABI

UNITED ARAB EMIRATES

**ARDIAN CANADA**

TEL: (+1) 212 641 8604

1250 RENÉ-LÉVESQUE OUEST
SUITE 4010
QC H3B 4W8 MONTRÉAL

CANADA

# APPENDIX 3 - MATERIAL SCOPE OF THE BCR

## 1. Management of internal activity audits

1. These Binding Corporate Rules apply to the processing related to the management of internal activity audits and to the management of audit recommendations.

2. The purpose of the transfer is the transfer the audit report in order to implement corrective measures.

3. Data are currently transferred from France, England, Germany, Switzerland, Italy, Jersey, Luxembourg to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:

- transmission;
- implementation of corrective measures;
- consultation;
- recording.

5. The categories of data subjects concerned by the transfers are the employees of Ardian.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details);
- professional life (professional phone number, email address, job title, business activities information and data contained in applications and tools provided to employees to conduct their business activities where it is in scope of the given audit, HR file data such as salary, benefits and expenses in the event it is in scope of an audit);
- categories of data listed in appendices 2 to 20 of the BCR as they relate to their assigned processing activities in the event the given process is in scope of an audit conducted by the Internal Audit Team.

7. The categories of data recipients are the employees of subsidiaries and sister companies.

8. The storage period of the data is the period of the audit increased by the period required for the implementation of the corrective actions.

# 2. Management of internal, external communication and of Corporate Development

1. These Binding Corporate Rules apply to the processing related to the management of Ardian's communication both for its internal and external communication and for the development of its Corporate Development activity.

2. The purpose of the transfer is the management of Ardian's communication.

3. Data are currently transferred between the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:
- consultation;
- recording;
- entry.

5. The categories of data subjects concerned by the transfers are the employees of Ardian as well as its (current or potential) customers.

6. The categories of data transferred are:
- data on identification (first name, last name, contact details);
- professional life (professional email address, job position, work projects, professional profile and career highlights, work background, pictures and videos where relevant and where consent is provided);
- personal life (personal life experience or circumstances where shared by the data subject if relevant to articles);
- economic and financial data (expenses and bank details for transactions where relevant as they relate to managing events the data subject takes part in);
- location data (place of the travel and of the event organized, flight details, hotel booking);
- religious beliefs (indication of specific dietary pattern that may reveal the religion of the data subjects).

7. The categories of data recipients are the employees of the subsidiaries and sister companies of Ardian in charge of the communication.

8. The storage period of the data is the period required to organize and carry out the event.

# 3. Management of knowledge and documentation

1. These Binding Corporate Rules apply to the processing related to the following up of subscriptions or online databases, the consultation of legal information on companies as well as to the management of subscriptions to specialized magazines.

2. The purpose of the transfer is the accessibility to the knowledge and documentation database as well as the management of the access codes to the different online information websites.

3. Data are currently transferred between the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:
- consultation;
- recording;
- download.

5. The categories of data subjects concerned by the transfers are the employees of Ardian.

6. The categories of data transferred are:
- data on identification (first name, last name, employee ID, usernames and logins to subscriptions where applicable);
- professional life (professional email address, job position, professional magazine and databases subscriptions and their corresponding access codes).

7. The categories of data recipients are the employees of subsidiaries and sister companies of Ardian.

8. The storage period of the data is the period of the validity of the data, in particular equivalent to the duration of the subscriptions taken out by Ardian.

# 4. Management of customers and investor relations

1. These Binding Corporate Rules apply to the processing related to the management of customers and investor relations.

2. The purpose of the transfer is to manage customers and investor relations according to their geographic activity area.

3. Data are currently transferred between the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:
- consultation;
- entry;
- recording.

5. The categories of data subjects concerned by the transfers are the employees of Ardian, its customers and its investors.

6. The categories of data transferred are:
- data on identification (first name, last name, investor or customer ID, usernames;
- professional life (professional email address, professional phone number, job position, company name);
- personal life (where relevant home address, phone number, family relationships relevant to investments);
- economic and financial data (bank details, transaction and financial history, investments, tax information).

7. The categories of data recipients are the employees of subsidiaries and sister companies of Ardian.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.

# 5. Management of customers invoicing, costs, reinvoicing and reporting

1. These Binding Corporate Rules apply to the processing related to the management of Ardian's accounting for the invoicing of its customers, the management of costs of boards of directors, the management of reinvoicing as well as reporting.

2. The purpose of the transfer is to manage and follow up the invoicing of funds, manage and follow up the costs of consultative committees as well as of the reporting.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:

- consultation;
- financial operations;
- entry.

5. The categories of data subjects concerned by the transfers are the employees of Ardian working on the file, customers and shareholders.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details);
- professional life (professional email address, phones number and address, job position, details of professional matter related to invoice);
- economic and financial data (expenses, invoices, cost details, bank details, transactions, confirmation of payment).

7. The categories of data recipients are the employees of subsidiaries and sister companies of Ardian and the customers (recipients of the invoices related to them).

8. The storage period of the data is the period required for invoicing operations.

# 6. Electronic document management

1. These Binding Corporate Rules apply to the processing related to electronic management of the documentation linked to Ardian's activity.

2. The purpose of the transfer is the electronic document management within a common work space.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:

- consultation;
- entry:
- recording.

5. The categories of data subjects concerned by the transfers are the employees of Ardian as well as the consultants of the EDM maintenance provider.

6. The categories of data transferred are:

- data on identification (first name, last name, user ID);
- professional life (professional email address, job position, documents assigned to user, documents management metadata related to user);
- connection data (records of document accesses, edits, and general document management audit trail).

7. The categories of data recipients are the employees of Ardian in charge of the electronic document management as well as those having access to the common work spaces.

8. Data are stored for as long as the records in which they are contained are stored. The storage period of such records is related to the retention period of documents classified electronically, i.e. 3 years for "Notices", "Report" and "Others", 10 years for documents of the "Legal" type.

# 7. Management of IT resources

1. These Binding Corporate Rules apply to the processing related to the management of IT resources, the optimization of maintenance, the assistance to users and the development of information centralized on the application for the management of IT equipment.

2. The purposes of the transfer are the management of IT resources and incidents.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:

- consultation;
- performance of actions required for the maintenance of IT resources.

5. The categories of data subjects concerned by the transfers are the employees of Ardian.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details, employee user ID);
- professional life (professional email address, job position, office location, devices assigned to user, details of access rights, details of incidents relating to IT resources of user where relevant, data on or derived from the use of tools provided to employees and Ardian's information systems, application data and data contained in applications that employees use in the course of their work).

7. The categories of data recipients are the departments of the subsidiaries and sister companies of Ardian in charge of managing IT resources.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.

# 8. Management of IT department activity

1. These Binding Corporate Rules apply to the processing related to the management of the internal organization of the IT department.

2. The purpose of the transfer is the management of organization of the IT department of Ardian.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:

- consultation.

5. The categories of data subjects concerned by the transfers are the employees of Ardian as well as the consultants of the application maintenance provider.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details, employee user ID);
- professional life (professional email address, job position, office location, details of participation in IT projects, details of participation in IT-related trainings, data on or derived from the use of tools provided to employees and Ardian's information systems, application data and data contained in applications that employees use in the course of their work).

7. The categories of data recipients are the departments of the subsidiaries and sister companies of Ardian in charge of managing the IT department.

8. The storage period of the data is the period of the projects implemented by the IT department.

# 9. Management of IT equipment and electronic mail service

1. These Binding Corporate Rules apply to the processing related to the management of IT equipment and electronic mail service.

2. The purposes of the transfer are the management of IT equipment as well as the management of the electronic mail service.

3. Data are currently transferred between the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operation made by the data recipients is the consultation of information.

5. The categories of data subjects concerned by the transfers are the employees of Ardian.

6. The categories of data transferred are:
- data on identification (first name, last name, contact details, employee user ID);
- professional life (professional email address, mailbox account details, user roles and distribution lists details and access rights, authentication data, job position and department, office location, communications, emails metadata, email configuration and troubleshooting information as relevant, user device information, data on or derived from the use of company electronic mail service provided to employees).

7. The categories of data recipients are the subsidiaries and sister companies of Ardian.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.

# 10. Management of disputes

1. These Binding Corporate Rules apply to the processing related to the defense of rights of Ardian in courts.

2. The purpose of the transfer is to manage the litigations in which Ardian, its subsidiaries or sister companies and/or its funds are a party, in particular in order to comply with the obligations required to establish, exercise or defend a legal right.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the management and follow up of disputes.

5. The categories of data subjects concerned by the transfers are the parties to the disputes, the opponent attorneys and the legal counsels or experts.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details, dispute reference numbers);
- professional life (professional email address, job position, office location, and the following where relevant to a particular dispute: business records, career progression, qualifications, details of participations in work projects, work performance, complaints, HR matters where applicable);
- economic and financial data (claims, settlement details if any, legal costs and where relevant to a particular dispute: expenses, invoices, cost details, bank details, transaction history, confirmation of payment, investments, tax information);
- offences;
- convictions;
- security measures.

7. The categories of data recipients are the legal departments of the subsidiaries and sister companies of Ardian.

8. Data are stored until exhaustion of remedies.

# 11. Management of legal secretariat

1. These Binding Corporate Rules apply to the processing related to the management of the legal secretariat by the legal department of Ardian.

2. The purpose of the transfer is the transmission for information purposes of the meeting reports of boards and other committees.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operation made by the data recipients is the consultation.

5. The categories of data subjects concerned by the transfers are the participants to boards and other committees.

6. The categories of data transferred are:

- data on identification (first name, last name);
- professional life (professional email address, job position, office location, details of work projects, participation to boards and other committees, reports with details of presentations, minutes and attendance).

7. The categories of data recipients are the departments concerned of the subsidiaries and sister companies of Ardian as well as the auditors.

8. Data are stored for the duration of Ardian.

# 12. Centralized management of current affairs for Investment team activity

1. These Binding Corporate Rules apply to the processing related to centralized management of current investment affairs.

2. The purposes of the transfer are:
- the centralized management of investment opportunities handled by investment teams;
- the entry of elements for the performance of funds-of-funds portfolio diversification.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates.

4. The processing operations made by the data recipients are the following:
- consultation;
- entry of data in the centralized database.

5. The categories of data subjects concerned by the transfers are the employees of Ardian, their current or potential customers as well as the investors.

6. The categories of data transferred are:
- data on identification (first name, last name);
- professional life (professional email address, job position, office location, details of participation in investment projects)
- economic and financial data (investment details, investment interests, subscription to funds, details of portfolio diversification, investment history).

7. The categories of data recipients are the members of the teams working on the current affairs for investment activities.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.

# 13. Management and follow up of the files assigned to Investment teams

1. These Binding Corporate Rules apply to the processing related to the management and follow up of the files assigned to the investment teams.

2. The purpose of the transfer is to follow up current affairs of investment activities.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates.

4. The processing operations made by the data recipients are the following:

- consultation.

5. The categories of data subjects concerned by the transfers are the employees of Ardian, their current or potential customers as well as the investors.

6. The categories of data transferred are:

- data on identification (first name, last name, professional email address);
- professional life (professional email address, job position, office location, details of participation in investment projects, data on or derived from the use of tools provided to employees from investment teams for the management of file, application data and data contained in applications that employees from investment teams use in the course of their work to manage and follow up files assigned to them);
- economic and financial data (investment details, investment interests, subscription to funds, details of portfolio diversification, investment history).

7. The categories of data recipients are the members of the teams working on the current affairs for investment activities.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.

# 14. Management of the activity of the Fund Finance teams

1. These Binding Corporate Rules apply to the processing related to the management and follow up of the files assigned to the Fund Finance teams.

2. Data are transferred to the USA, Switzerland and Germany for the management of local funds. Data are transferred to all of the subsidiaries/sister companies for the management of all of the Fund Finance activities and in particular the following up of portfolio shareholdings and the preparation of valorization committees. Lastly, data are transferred to auditors and fund administrators established in Jersey and Luxembourg for the purposes of invoicing and preparing evaluation committees.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates.

4. The processing operations made by the data recipients are the following:

- the consultation;
- the entry of data in the centralized database;
- the performance of financial operations.

5. The categories of data subjects concerned by the transfers are the employees of Ardian, their current or potential customers, the investors as well as the contact persons of providers and portfolio companies.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details);
- professional life (professional email address, job position, details of portfolio shareholdings, participation and work related to valorization and evaluation committees);
- economic and financial data (invoice details, payment information, transaction history, investment details, investment interests, subscription to funds, bank details, investment history).

7. The categories of data recipients are the departments concerned of the subsidiaries and sister companies of Ardian and auditors.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.

# 15. Management of personal transactions

1. These Binding Corporate Rules apply to the processing related to the management, follow up and control of the personal transactions of employees in accordance with the regulations governing the activity of Ardian.

2. The purposes of the transfer are to follow up and issue authorizations for the personal transactions of employees.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operation made by the data recipients is the consultation.

5. The categories of data subjects concerned by the transfers are the employees of Ardian.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details);
- professional life (professional email address, professional phone number, job position, data relating to criminal background as may be relevant to the prevention of market abuse or conflicts of interest);
- economic and financial data (personal transaction details and history, information notified to the employer to prevent market abuse or conflicts of interest, professional suitability and probity, data relating to salary, benefits and expenses, data relating to holdings of private securities, and investments).

7. The categories of data recipients are the services concerned of the subsidiaries and sister companies of Ardian.

8. The storage period of the data is 5 years from the declaration of the personal transactions.

# 16. Fight against money laundering and the financing of terrorism

1. These Binding Corporate Rules apply to the processing related to the fight against money laundering and the financing of terrorism.

2. The purpose of the transfer is to fight against money laundering and the financing of terrorism in accordance with the statutory and regulatory provisions of Ardian and any international agreement signed in that respect.

3. Data are currently transferred from France, Germany, Switzerland, Italy, Jersey, Luxembourg and the United Kingdom to the following countries:

- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:

- consultation;
- entry, if applicable.

5. The categories of data subjects concerned by the transfers are the current or potential customers or investors.

6. The categories of data transferred are:

- data on identification (first name, last name, contact details, copy of ID or passport);
- professional life (professional email address, professional phone number, job position, company);
- personal life (proof of address, date of birth, relationship with signatories and ultimate beneficial owner where relevant);
- economic and financial data (source and origin of funds, details of business or employment, disclosures made from data subjects if any).

7. The categories of data recipients are the departments concerned of Ardian.

8. The data are stored as follows:

- data related to operations made by customers which are registered for the fight against money laundering and the financing of terrorism are stored for five years from the year in which the operation is made, including in case the customer account is closed or the relations are ended;
- data related to measures to freeze funds are stored for a period that cannot exceed the period during which those measures are applicable.

9. In case of a request by a foreign authority concerning fight against money laundering and involving a transfer of personal data to that authority in application of the local law, internal procedures are implemented in order to protect the data and inform the competent data protection authorities concerned.

# 17. Management of recruitment operations

1. These Binding Corporate Rules apply to the processing related to the management and follow up of recruitment operations within Ardian.

2. The purpose of the transfer is to follow up job applications.

3. Data are currently transferred between the following countries
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operation made by the data recipients is the consultation of job applications.

5. The categories of data subjects concerned by the transfers are the job applicants.

6. The categories of data transferred are:
- data on identification (first name, last name, contact details, copy of ID or passport);
- professional life (job position, career history, CV, references, education history, trainings, job application and interview details, onboarding documents and signed contract where applicable);
- economic and financial data (current and expected salary, details of bonuses and other benefits).

7. The categories of data recipients are the departments concerned of the subsidiaries and sister companies of Ardian.

8. The data are stored as follows:
- data related to recruitment procedures are in principle stored 2 years after the last contact with the job applicant;
- in case of claim/complaint about a negative answer made to a job applicant within that period, all of the documents justifying the refusal decision are kept for a period of 5 years after the sending of the negative answer to the job applicant.

# 18. Management of personnel work organization

1. These Binding Corporate Rules apply to the processing related to the management of personnel work organization of Ardian.

2. The purpose of the transfer is to organize personnel work within Ardian.

3. Data are currently transferred between the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Korea;
- Jersey;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:
- consultation;
- entry.

5. The categories of data subjects concerned by the transfers are the employees of Ardian.

6. The categories of data transferred are:
- data on identification (first name, last name);
- professional life (professional email address, professional phone number, job position, office, information relating to professional calendar, mailbox, company intranet, data on or derived from the use of tools provided to employees and Ardian's information systems, application data and data contained in applications that employees use in the course of their work, data relating to absences and leaves, business travel information where applicable, workload, details of projects assigned to employee).

7. The categories of data recipients are the departments concerned of the subsidiaries and sister companies of Ardian.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.

# 19. Administrative management of personnel

1. These Binding Corporate Rules apply to the processing related to the administrative management of Ardian's personnel, the following up of its training programs, and the management of its mobility and career.

2. The purpose of the transfer is to carry out the administrative management of Ardian's personnel, follow up its training programs and manage its mobility and career.

3. Data are currently transferred between the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:
- consultation;
- entry.

5. The categories of data subjects concerned by the transfers are the employees of Ardian.

6. The categories of data transferred are:
- data on identification (first name, last name, contact details);
- professional life (professional email address, job position, office, manager, appraisal, career progression, trainings, mobility requirements, information relating to leaves of absences);
- economic and financial data (data relating to tax and pension, salary, bonus and other compensation details, bank details, payments, payslips, expenses and claims).

7. The categories of data recipients are the departments concerned of the subsidiaries and sister companies of Ardian.

8. The data are stored as follows:
- administrative following up staff records within the company are stored for the period of the contractual relationship;
- data related to grounds of leaves of absences are for no longer than is necessary for the establishment of payslips;
- data related to particular constraints entitling to special leaves of absence or time-off rights for staff representation are not stored beyond the period of constraint of the employee concerned.

# 20. Management and following up of complaints and incidents

1. These Binding Corporate Rules apply to the processing related to the management of incidents and complaints from Ardian's customers.

2. The purpose of the transfer is to manage incidents and complaints from customers.

3. Data are currently transferred between the following countries:
- Chile;
- China;
- France;
- Germany;
- Italy;
- Japan;
- Jersey;
- Korea;
- Luxembourg;
- Singapore;
- Spain;
- Switzerland;
- United Kingdom;
- USA;
- United Arab Emirates;
- Canada.

4. The processing operations made by the data recipients are the following:
- consultation;
- entry;
- resolution of incidents.

5. The categories of data subjects concerned by the transfers are the employees of Ardian, its customers and investors.

6. The categories of data transferred are:
- data on identification (first name, last name, contact details, information in scope of complaint or incident);
- professional life (professional email address, job position, relationship with Ardian, record and outcome of complaint or incident);
- economic and financial data (payments and financial transactions, payment failure, payment due date, specific financial information as it relates to complaint or incident).

7. The categories of data recipients are the departments concerned of the subsidiaries and sister companies of Ardian.

8. The storage period of the data is the period of the contractual relation increased by the term of the statute of limitations.