HERMES GROUP

Binding Corporate Rules (BCRs) for intra-group transfers of personal data to non-EEA countries

April 2020

SUMMARY

1. PURPOSE OF THE BCRs

HERMES GROUP is committed to ensure the highest possible level of customer care and to ensure customers trust. In this context, customers' right to privacy is a prime consideration for HERMES GROUP.

Under the provisions of the "Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation or "GDPR") repealing Directive 95/46/EC", any Transfer of Personal Data outside the European Economic Area (EEA) shall be framed by specific safeguards, with a view to make the use of Personal Data compliant with European Data Protection Principles (defined in section 2). Thus, the adoption and the implementation of Binding Corporate Rules (BCRs) within the HERMES GROUP will aim to regulate intra-group Data Transfers related to Personal Data processed by the HERMES GROUP outside the European Economic Area (EEA), in accordance with the provisions of the GDPR and the 2002/58 EU Directive and any other related laws and regulations applicable in Europe.

HERMES GROUP perceives these BCRs as an essential tool to effectively promote our culture on data protection within the HERMES GROUP. These BCRs will also foster data protection compliance and ease the management of Personal Data within the whole group.

Beyond, HERMES GROUP and its Employees are responsible for protecting and respecting personal information to which they have access. Therefore, we believe that our BCRs are an essential tool to effectively manage this important responsibility and to broadcast and share our culture on Privacy within the Group.

With regard to the scope of our BCRs, HERMES GROUP entities which adhere to the BCRs and Employees of the HERMES GROUP shall comply with the following provisions, as well as with Applicable Data Protection Law. HERMES GROUP has set up an effective governance structure to manage such data protection obligations.

At local level, and according to the terms of our BCRs, each Local Data Controller will have to sign a BCRs agreement and shall take every necessary step on a day to day basis to ensure compliance with the provisions of the BCRs. Compliance with these provisions and procedures will especially rely on training programs and auditing activities.

Because of their wide scope in terms of Data Protection compliance, the use of BCRs at local level will, without any doubt, ease the management of Data Protection compliance and will help to ensure that local representatives take ownership of data protection.

Would a violation of the BCRs be established, any corrective measure (legal, technical or organizational measure) as well as any appropriate sanction (against the Local Data Controller or, according to local labor law, a local Employee) may be taken on the initiative of the Head Controller, the Global CRM Manager, the Global Privacy Office, the Local Data Controller or the local CRM Manager.

2. DEFINITIONS AND DATA PROTECTION PRINCIPLES

2.1. DEFINITIONS

The terms and expressions used in the BCRs are defined in appendix 1, provided that these terms and expressions shall always be interpreted according to the GDPR and the 2002/58 Directive.

2.2. DATA PROTECTION PRINCIPLES

Within the scope of the BCRs (see paragraph 3), any Transfer of Personal Data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, defined in specific paragraphs of the BCRs or in appendix 2, in accordance with the provisions of the GDPR and 2002/58.

- **Fairness and Transparency of the Processing**: Fairness requires that the Data Subject shall be informed of the existence of the Processing operation and its purposes. Any information relating to the Processing of the Data Subjects' Personal Data shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language (see Appendix 2).
- **Lawfulness**: In order for Processing to be lawful, the Processing of Personal Data shall be processed on the basis of the Consent of the Data Subject concerned or some other legitimate basis, including the necessity for compliance with the legal obligation to which the Controller is subject, etc. (see Appendix 2).
- **Purpose limitation**: Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (see Appendix 2).
- **Data Minimization**: Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or processed (see Appendix 2).
- **Data quality**: Personal Data shall be accurate and, where necessary, kept up to date (accuracy) (see Appendix 2)
- **Limited Storage Periods:** Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (see Appendix 2).

- **Data protection by design / Data protection by default**: It is necessary to implement appropriate Technical and Organizational Measures, which are designed to implement these Data Protection principles, in an effective manner and to integrate the necessary safeguards into the Processing. These measures have to ensure that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed (see Appendix 2)
- **Security and confidentiality**: appropriate Technical and Organizational Measures shall be implemented to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing (see paragraph 4.5).
- **Onward Transfers to organizations not bound by BCRs:** HERMES GROUP shall implement adequate safeguards when Personal Data is intended to be transferred to a non-HERMES entity (see paragraph 5.6 and Appendix 2).
- **Accountability**: The Local Data Controller shall be responsible for, and be able to demonstrate compliance with the above Data Protection Principles.

3. SCOPE OF THE BCRs

3.1. GEOGRAPHICAL SCOPE

The BCRs shall apply to Transfers of Personal Data between entities of the HERMES GROUP established throughout the world and which have signed the BCRs, or a BCR intra-group agreement

Appendix 3 gives a list of all HERMES GROUP entities bound by the BCRs.

3.2. MATERIAL SCOPE

The nature and purposes of the Personal Data being transferred within the scope of the BCRs is detailed in appendix 4.

3.3. SCOPE OF ENTITIES COVERED

The purpose of these BCRs is to frame intra-group Transfers of Personal Data between those HERMES GROUP entities listed in Appendix 3, who act either as Local Data Exporters or as Local Data Importers.

All HERMES GROUP entities undertake to abide by these BCRs upon signature of the BCR Intra-Group Agreement (Appendix 5).

4. EFFECTIVENESS OF THE BCRs

4.1. TRANSPARENCY AND INFORMATION RIGHT

To make the Data Processing fair, Personal Data shall always be collected and further processed on a transparent basis. Thus:

1. The BCRs shall always be readily available to every Data subject and therefore shall be uploaded on HERMES GROUP internet and intranet websites. A Data subject shall always be able to obtain, upon request, a copy of the BCRs from the Local CRM manager, the Local Data Controller, the Global CRM Manager or the Global Privacy Office. HERMES GROUP will also provide Data Subjects with the following information:
   a. Information on their third party beneficiary rights with regards to the Processing of their Personal Data and on the means to exercise those rights (see paragraph 5.3 below);
   b. Information on the clause relating to the liability (see paragraph 5.4 below);
   c. Information on the data protection principles (see Appendix 2);
   d. Information upon request of the essence of the arrangement of Joint-Controller relationship (if any) (see also paragraph 5.6 below).

2. Furthermore, specific FAQs shall be available for customers on HERMES GROUP internet websites, with a view to clarify any question Data Subjects may have about the BCRs or any related matter, such as concerns or requests related to submitting an access request to their Personal Data (see paragraph 5.2) or submitting a claim (see paragraph 5.3).

3. Data Subjects are entitled to be informed of the Processing of their Personal Data. Local CRM managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall be able to provide templates of notices to every Local Data Controller within the Group, for any purpose that requires information to be made to the Data Subjects.

4. Where, with regard to an existing Processing, a new purpose or a new category of Recipient arises, the appropriate information notice shall be consequently modified and the relevant Data Subjects shall be informed of such modification.

5. HERMES GROUP will provide a Data Subject with at least the following information, except where he already has it:
   a. the identity and contact details of the Local Data Controller and of his representative, if any,

b. the contact details of the appointed data protection Officer, if any;
c. the purposes of the Processing for which the data are intended, as well as the legal basis for the Processing;
d. the legitimate interests pursued by the Local Data Controller or by a Third Party (when the Processing is based on this ground);

e. the Recipients or categories of Recipients of the data;
f. where applicable, the fact that the Local Data Controller intends to transfer Personal Data to a third country, and the details of the relevant safeguards, including the existence or absence of an adequacy decision by the European Commission , and the means by which to obtain a copy of them or where they have been made available;
g. the period for which the Personal Data will be stored (or the criteria used to determine that period);
h. the existence of the right to request from the Local Data Controller access to and rectification or erasure of Personal Data or restriction of Processing or to object to Processing as well as the right to data portability where such right is applicable;
i. where the Processing is based on the Data Subject's Consent either as lawful basis for the Processing or for Processing of Special Categories of Personal Data, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before withdrawal;
j. the right to lodge a complaint with a Supervisory Authority;
k. whether the provision of Personal Data is statutory or contractual, whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
l. the existence of Automated Individual Decision Making, including Profiling, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
m. the intention to further process the Personal Data for a purpose other than for which it was collected;
n. from which source the Personal Data originates and if applicable whether it came from publicly accessible source (where Personal Data has not been obtained directly from the Data Subject).

Processing

Where the data has not been directly obtained from the Data Subjects, HERMES GROUP will provide the relevant Data Subjects with the information above within a reasonable period after obtaining the Personal Data, but at the latest within one month, taking into consideration to the specific circumstances under which the Personal Data are processed. If the Personal Data are to be used for communication with the Data Subject, such information will be provided at the latest at the time of the first communication to that Data Subject; or if a disclosure to another Recipient is envisaged, at the latest when the Personal Data are first disclosed.

However, according to Article 14(5) of the GDPR, which applies where the Personal Data have not been directly obtained from the Data Subjects and notwithstanding any specific provision set out in national legislations, this disclosure of information to the Data Subject will exceptionally not apply (i) where the Data Subject already has the information, (ii) where the provision of such information proves impossible or would involve a disproportionate effort or (iii) if obtaining or disclosure is expressly laid down by law to which the Data Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests or (iv) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by law (including a statutory obligation of secrecy).

4.2. RIGHTS OF ACCESS, RECTIFICATION, ERASURE, RESTRICTION OF PROCESSING, TO OBJECT TO THE PROCESSING AND TO DATA PORTABILITY

Data Subjects are entitled to be told what information HERMES GROUP holds on them and to keep this information under control. Thus:

1. Every Data Subject has the right to (after having established his identity and made specific request to HERMES GROUP):

a. **Obtain from HERMES GROUP without constraint at reasonable intervals and without excessive delay or expense**:
- confirmation as to whether or not Personal Data relating to the Data Subject is being processed;
- if the former is the case, information as to the elements g), i), k), l), n), p) and r) under paragraph 4.1.5 above;
- where Personal Data are transferred to a third country, information about the appropriate safeguards used for the Data Transfer;
- communication to him in an intelligible form of the data undergoing Processing and of any available information as to their source.
-

b. **Obtain from HERMES GROUP without undue delay - the rectification, of inaccurate Personal Data, concerning him or her.** Taking into account the purposes of the Processing, the Data Subject has the right to have incomplete Personal Data completed, including by means of providing a supplementary statement;

c. **Obtain from HERMES GROUP, without undue delay, the erasure of Personal Data concerning him or her where one of the following grounds applies**: i) where the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; ii) where the Data Subject withdraws Consent on which the Processing is based and there is no other legal ground for the Processing and there are no overriding legitimate grounds for the Processing; iii) the Data Subject objects to the Processing in accordance with point g. below when there are no overriding legitimate grounds for the Processing or the Data Subject objects to the Processing for the purposes of direct marketing in accordance with point h. below; iv) the Personal Data has been unlawfully processed; v) the Personal Data has to be erased for compliance with a legal obligation to which HERMES GROUP is subject; vi) the Personal Data has been collected in relation to the offer of information society services which cover any service, normally provided for remuneration, at a distance, by means of electronic equipment for the Processing and storage of data;

Where HERMES GROUP has made the Personal Data processed public and is obliged to erase the Personal Data, HERMES GROUP will take reasonable steps, including technical measures, to inform any Controllers Processing the Personal Data concerned that the Data

Subject has requested the erasure of any links to, or copy or replication of, those Personal Data (taking account of available technology and the cost of implementation) and request that such Controller comply with this request

However, exceptions to this right to erasure apply i) when the Processing is necessary for exercising the right of freedom of expression and information; ii) for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; iii) 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; for the establishment, exercise or defense of legal claims;

d. **Obtain from HERMES GROUP restriction of Processing** where one of the following grounds applies: i) when the accuracy of the Personal Data is contested (for the period necessary to verify the accuracy of the data), ii) when the Processing is unlawful and the Data Subject requests the restriction of their use, iii) when HERMES GROUP no longer needs the Personal Data Processing but they are required by the Data Subject for the establishment, exercise or defense of legal claims and iv) when the Data Subject has objected to a Processing HERMES GROUP has based on the legitimate interest of HERMES GROUP (for the period necessary to verify whether the legitimate grounds of HERMES GROUP override those of the Data Subjects if applicable);

e. **Obtain from HERMES GROUP that HERMES GROUP shall notify third parties to whom the Personal Data have been disclosed of any rectification, erasure or restriction carried out in compliance with (b), (c), (d)** unless this proves impossible or involves a disproportionate effort. The Local Data Controller shall inform the Data Subject about those third parties if the Data Subject requests it;

f. **Exercise his or her right to data portability** and obtain from HERMES GROUP the right to receive communication of his or her Personal Data, which he or she has provided to HERMES GROUP, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from HERMES GROUP, when the Processing is based on Consent or on a contract and the Processing is carried out by automated means;

g. **Object at any time on compelling legitimate grounds** relating to the Data Subject's particular situation **to the Processing** of Personal Data (based on the legitimate interest of HERMES GROUP)relating to the Data Subjects.

According to the GDPR, the exercise of those rights may be subject to certain limitations, in particular Local Data Controllers may object to requests that are obviously excessive, in particular by their number, or their repetitive and systematic character;

h. **Object, at any time of the Processing, free of charge, and without having to state legitimate grounds, to the Processing of Personal Data** for the purposes of direct marketing including Profiling, or to be informed before Personal Data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

2. Specific guidelines and procedures shall be in place within the Group, at local level, to ensure the exercise of the rights specified above. In particular, HERMES GROUP Employees who collect, process or have access to Personal Data shall be trained to recognize a Data Subject access, rectification, erasure, restriction, objection or portability request. Each request shall be acknowledged and handled according to the local procedure in place.

3. A specific answer shall be systematically given to the Data Subject within a reasonable period of time (i.e., no later than one month of receipt of the request). That period may be extended by two further months where necessary taking into account the complexity and number of the requests. HERMES GROUP shall inform the Data Subject of any extension within one month of receipt of the request together with the reasons for the delay.

4. If the request is found legitimate, HERMES GROUP shall take any necessary step to handle the matter in due time. If the request is denied, the reason for denial shall be communicated in writing (or by email) to the Data Subject. In such a case, the Data Subject may follow the internal complaint mechanism specified in paragraph .4.

5. Local CRM managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall always be at the disposal of both Local Data Controllers and Data Subjects to assist them in relation to Data Subjects' requests when necessary.

4.3. AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

1. Subject to Applicable Data Protection Law, every Data Subject has 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 significantly affects him or her.

2. The above does not apply if the decision:
   - is necessary for entering into, or performance of, a contract between the Data Subject and HERMES GROUP;
   - is authorized by Applicable Data Protection Law to which HERMES GROUP is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests;
   - or is based on the Data Subject's explicit Consent.

4.4. INTERNAL COMPLAINT MECHANISM

1. If a Data Subject believes that its Personal Data is not processed in accordance with the BCRs or the Applicable Data Protection law, the

Data Subject may lodge, in accordance with the BCRs Complaint Procedure, a complaint to any of the following stakeholders, whose independence is guaranteed during the performance of their functions (for instance the local Data Protection Officer).

2. Specific guidelines and procedures shall be in place within the Group, at local level, to ensure a complaint mechanism to be consistent and to ensure sufficient information to be provided to the Data Subjects about these procedures. When a complaint is registered, it must be acknowledged and handled within a reasonable period of time (i.e., no later than one month of receipt of the request. That period may be extended by two further months where necessary taking into account the complexity and number of the requests. HERMES GROUP shall inform the Data Subject of any extension within one month of receipt of the request together with the reasons for the delay).
3. All HERMES GROUP representatives and Employees shall, at local level, do their best efforts to help the Local Data Controller or the Local CRM Manager to settle a complaint . All data protection complaints received by a Local Data Controller or any Employee shall be communicated to the relevant Data protection contact(s) without any delay.

4. If the Hermes Group representatives fail to solve the claim at local level, the complaint handling mechanism shall allow escalating the problem to the Global CRM Manager or the Global Privacy Office which shall respond within no later than one month of receipt of the request. That period may be extended by two further months where necessary taking into account the complexity and number of the requests. HERMES GROUP shall inform the Data Subject of any extension within one month of receipt of the request together with the reasons for the delay.

5. Each HERMES GROUP entity subject to these BCRs shall have on its Internet website – if available - practical tools allowing Data Subjects to lodge their complaints, including at least one of the below:
    a. Email address
    b. Telephone number
    c. Postal address

6. Each Local Data Controller and local CRM manager shall regularly report to the Legal Global CRM Manager and the Global Privacy Office about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of Data Protection compliance.

7. For avoidance of doubt, it is understood that if the Data Subject is not satisfied by the replies of Hermes Group representatives at local and global level or if the Data Subject prefers to bypass the available internal complaint mechanism, the Data Subject has the right to lodge a complaint before the relevant Supervisory Authority (where the GDPR is applicable, in the EU Member State of his habitual residence, of his place of work or place of the alleged infringement) and/or before the competent jurisdictions (where the GDPR is applicable, the court of the Member State where the Local Data Controller has an establishment or where the Data Subject has his habitual residence) (see paragraph 5.3).
   Prior to referring a case to the relevant Supervisory Authority or competent jurisdiction, the Data Subject shall be informed of the possibility to solve a claim through the internal complaint mechanism described above and the BCRs Complaint Procedure.

4.5. SECURITY AND CONFIDENTIALITY / RELATIONSHIPS WITH PROCESSORS THAT ARE MEMBERS OF THE GROUP

4.5.1. General security and confidentiality principles

Ensuring that personal information is appropriately protected from Personal Data Breaches is a HERMES GROUP top priority. Thus:

1. Each Local Data Controller shall implement appropriate Technical and Organizational Measures to protect Personal Data against Personal Data Breach taking into consideration the state of art of technology and the cost of implementation , the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects.

   Furthermore, the implemented measures shall ensure (i) a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, such as including, where appropriate, the Pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of Technical and Organizational Measures for ensuring the security of the Processing.

   Consequently, appropriate information security policies and procedures shall be designed and implemented within the Group. These security policies set up all appropriate physical and logical measures with a view to prevent or deter accidental destruction, modification or unauthorized disclosure or access to pPersonal Data. These policies and procedures shall be regularly audited (see paragraph 4.9).

2. Special Categories of Personal Data shall be processed with enhanced and specific security measures.

3. Access to Personal Data is limited to Recipients for the sole purpose of performing their professional duties. Disciplinary sanctions may occur if a HERMES GROUP Employee fails to comply with the appropriate information security policies and procedures.

4. In case of Personal Data Breach:
    - Notify any Personal Data Breach to the appointed data protection officer or data protection contact (e.g. Local CRM Managers) who will then notify the Head Controller, the Global CRM Manager and the Global Privacy Office without undue delay;
    - Document any Personal Data Breach (comprising the facts relating to the Personal Data Breach, its effect and the remedial actions taken) and make available the documentation to the Supervisory Authorities on request;
    - Notify the Personal Data Breach to the competent Supervisory Authority without undue delay and, where feasible, not later than

72 hours after having become aware of it, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

- Inform Data Subjects of any Personal Data Breach that could significantly affect them as well as the measures taken for its resolution.

4.5.2. Relationships with Processors that are members of the HERMES GROUP

Where a Local Data Controller requests that another entity of the HERMES GROUP undertakes Processing of Personal Data on its behalf (for the purpose of Processing the type of Personal Data and categories of Data Subjects as described in Appendix 4 of the BCRs, but strictly for the subject matters and durations specified by the Local Data Controller) (for a short term period as well as for a long term period, depending on the case), the following safeguards shall be followed:

1. Where the Processing is carried out, the Local Data Controller shall choose a Processor providing sufficient guarantees in respect of the Technical and Organizational Measures governing the Processing to be carried out, and must ensure compliance with those measures. Any entity of HERMES GROUP which is bound by the BCRs by signing the BCR Intra-Group Agreement in Appendix 5 and acting as a Processor on behalf of a Local Data Controller undertakes to provide those sufficient guarantees in respect of the Technical and Organizational Security Measures governing the Processing to be carried out and to comply with all safeguards contained herein when acting as a Processor on behalf of a Local Data Controller and must ensure compliance with those measures. Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall be able to provide templates of the appropriate Data Processor clauses to a Local Data Controller within the Group.

2. The appointed entity of the HERMES GROUP (Processor) must not process the Personal Data except on instructions from the Local Data Controller, unless he is required to do so by law in which case the Processor shall promptly notify the Local Data Controller (unless prohibited by law or important grounds of public interest).

3. The appointed entity of HERMES GROUP (Processor) undertakes to:
    - To ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
    - Implement Technical and Organizational Security Measures to sufficiently protect the Personal Data against any data breach;
    - To respect the conditions for engaging another Processor (see below);
    - To assist the Local Data Controller, taking into account the nature of the Processing, by putting in place appropriate Technical and Organisational Measures, insofar as this is possible, for the fulfilment of the Local Data Controller's obligation to respond to requests for exercising the Data Subject's rights as indicated in paragraph 5.2 above;
    - To assist the Local Data Controller in ensuring compliance with its obligations as regards the security of Personal Data, the notification of a data breach, the data protection impact assessment and the prior consultation of the local Supervisory Authority (where necessary);
    - At the choice of the Local Data Controller, to delete or return all the Personal Data to the Local Data Controller after the end of the provision of services relating to Processing, and delete existing copies unless national law requires storage of the Personal Data;
    - To make available to the Data Controller all information necessary to demonstrate compliance with these obligations and allow and contribute to audits of its Processing activities including inspections, conducted by the Local Data Controller or another auditor mandated by the Local Data Controller;
    - To inform the Local Data Controller if in his opinion an instruction infringes the applicable data protection provisions;
    - To implement procedures for managing data breaches and to notify the Local Data Controller immediately after becoming aware of a Personal Data Breach and provide continuous assistance;
    - Allow the Local Data Controller, on request, to conduct an audit of its Processing activities to ensure that the Processor provides such sufficient security protections;
    - Not disclose Personal Data to any Third Party outside the HERMES GROUP without the prior explicit Consent of the Local Data Controller (see also paragraph 5.6 below regarding Transfers of data outside of the HERMES Group). In case of consented disclosure, the same data protection obligations as set out above will be imposed by the appointed of the HERMES GROUP entity (Processor) on that Third Party by way of a contract. Where such Third Party fails to fulfil its data protection obligations, the appointed HERMES GROUP entity (Processor) shall remain fully liable to the Local Data Controller for the performance of that other Third Party's obligations.

4. The Local Data Controller agrees that a HERMES GROUP entity acting as Processor may use another entity within the HERMES GROUP for sub-Processing. In this case, the initial Processor undertakes to inform the Local Data Controller of any intended changes concerning Processors, thereby giving the Local Data Controller the opportunity to object to such change.

5. If the Processor determines the purposes and means of a Processing, the Processor is considered to be a Data Controller in respect of that Processing.

6. The appointed entity of HERMES GROUP (Processor) must maintain a Record of Processing Activities concerning the Processing activities carried out on behalf of the Local Data Controller.

7. The appointed Processor will be held liable for any damage caused by the Processing where it has not complied with obligations of the BCR specifically applicable to Processors or where it has acted outside or contrary to lawful instructions of a Local Data Controller (except if it proves that it is not in any way responsible for the event giving rise to the damage).

8. Where both a Controller and a Processor (or more than one Controller or Processor), are involved in the same Processing and where they are responsible for any damage caused by Processing each Controller or Processor shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject. Where a Controller or Processor has paid full compensation for the damage suffered, that Controller or Processor shall be entitled to claim back from the other Controllers or Processors involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage.

4.6. RELATIONSHIPS BETWEEN JOINT CONTROLLERS THAT ARE MEMBERS OF THE HERMES GROUP

Where two or more Controllers within the HERMES GROUP jointly determine the purposes and means of Processing, they shall be Joint Controllers and they undertake the following:

1. To clearly describe and document the Processing operation carried out by each Joint-Controller concerning the Personal Data Processing concerned;

2. To implement the Personal Data Processing in compliance with the GDPR requirements and as reflected in the Records of Processing Activities and other documentation related to the Personal Data Processing (such as the data protection impact assessment);

3. To agree to inform each other before implementing any changes on the Personal Data Processing in order to analyze the impact of such change on the compliance of the Personal Data Processing and agree on the measures and conditions of implementation of said modification (e.g. modification of information notice), where so required;

4. To communicate to the Data Subjects upon request the essence of this arrangement and shall agree on the means used for this communication;

5. To decide which Joint-Controller will be in charge of the providing the information notice of to the Data Subject and of collection of Consent (when required) of the Data Subjects. On that matter, the Joint Controllers agree that the Joint Controller who will carry out the collection of the Data Subject will be in charge of these requirements;

6. That in case of request or claim of a Data Subjects, the Joint-Controller who has received the claim undertakes to inform the other Joint-Controller and to handle the request on behalf of the other Joint-Controller in compliance with the paragraph 4.4 (Internal complaint mechanism) and to keep the other Joint-Controller informed of the answers provided to the Data Subjects. The other Joint-Controller undertakes to provide reasonable assistance and cooperation, to allow the Joint-Controller to respond to requests or claims presented by Data Subjects;

7. That the Joint-Controller who is in charge of the collection of the Personal Data is in charge to establish and update (if needed) the Records of Processing Activities on behalf of all Joint-Controllers and to communicate this Records to other Joint-Controller upon request. The other Joint-Controller undertakes to provide with reasonable assistance and cooperation, to allow the establishment of the Records;

8. That the Joint-Controller who is in charge of the collection of the Personal Data is in charge to determine that a data protection impact assessment is required and if it is the case to:
    a. Inform the other Joint-Controller of this fact and complete a data protection impact assessment;
    b. Inform the other Joint-Controller with i) the result of the evaluation of the data protection impact assessment, ii) the proposed allocation of responsibilities of each Joint Controller with regard to the actions to be implemented and iii) whether or not prior consultation with the Supervisory Authority if necessary;

    The other Joint-Controller undertakes to provide reasonable assistance and cooperation concerning the performance and completion of the data protection impact assessment and to explicitly validate the decision/results of the data protection impact assessment, including an agreement by the Joint-Controllers to consult a Supervisory Authority;

9. That the Joint-Controller who is in charge of the collection of the Personal Data is in charge to conduct a data protection compliance assessment of the Personal Data Processing (where a data protection impact assessment is not necessary) and to inform the other Joint-Controller with i) the result of the compliance assessment and ii) the proposed allocation of responsibilities of each Joint Controller with regard to the actions to be implemented. The other Joint-Controller undertakes to provide with reasonable assistance and cooperation concerning the performance and completion of the compliance assessment and to explicitly validate the decision/results in relation with the data protection compliance assessment including the data retention periods to be implemented;

10. To preserve the security of the Personal Data Processing and to prevent against Personal Data Breach as provided by paragraph 4.5.1;

11. That the Joint Controller whose information system has been the victim of the Personal Data Breach (“the Affected Party”) will have to inform the other Joint-Controller and undertake to comply with paragraph 5.4.1 (e.g., notification to the appointed data protection officer, etc.). The Joint-Controllers commit to agree on the content of the notification to be sent to Supervisory Authority and to the Data Subjects in a timeframe compatible with the GDPR requirements. In case, the Personal Data Breach occurs in the Information System of a Processor (within or outside of the HERMES GROUP), the Parties agree that the Joint-Controller who has initiated the involvement of this Processor will be in charge with the Personal Data Breach management;

12. To comply with article 4.5.2 in case of sub-contracting within the HERMES GROUP. In that case the Joint-Controller would have also to inform the other Joint-Controller;

13. To comply with article 4.7 in case of Transfers to Processor and Controller outside the HERMES GROUP. In that case the Joint-Controller would have to obtain the prior written consent of the other Party. In addition, in case of sub-contracting outside the HERMES GROUP, the

Joint-Controller who initiates the involvement of the Processor will be in charge of the negotiation of the written agreement with the Processor or Controller which will be concluded on behalf of all the Joint Controllers (see also for more detail paragraph 4.7);

14. To document their respective obligations in relation with the Personal Data Processing as described in this paragraph and to make available upon request to the other Joint Controller within a reasonable time all the information and other documents requested as necessary to demonstrate compliance with its obligation;

15. To be audited by the other Joint-Controller in order to verify as to whether the other Joint-Controller complies with its obligations;

16. The Joint-Controllers are jointly responsible for any damage caused by Processing and each Joint-Controller shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject. Where one Joint-Controller has paid full compensation for the damage suffered, that Joint-Controller shall be entitled to claim back from the other Joint-Controller involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage.

4.7. RESTRICTIONS ON TRANSFERS AND ONWARD TRANSFERS TO EXTERNAL PROCESSORS AND CONTROLLERS

Where a Local Data Controller requests that a non-HERMES GROUP entity undertakes Processing of Personal Data as a Processor or a Controller, (an External Processor or an External Controller), the following safeguards shall be followed:

1. **External Processors located inside the EEA or in a country recognised by the EU Commission as ensuring an adequate level of protection** shall be bound by a written agreement stipulating that the processor shall act only on instructions from the Local Data Controller and shall be responsible for the implementation of the adequate security and confidentiality measures (see paragraph 5.4.). Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall be able to provide templates of the appropriate clauses to a Local Data Controller within the Group.

2. **All Transfers of Personal Data to External Controllers located out of the EEA** in a country not recognized by the EU Commission as ensuring an adequate level of protection must respect the European rules on transborder data flows (Articles 46 and 49 of the GDPR), for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission, standard data protection clauses adopted by a Supervisory Authority and approved by the EU Commission, an approved code of conduct, an approved certification mechanism, contractual clauses between the HERMES GROUP entity and the External Controller subject to authorization from the competent Supervisory Authority or derogations for specific situations. In addition, for Joint-Controllers relationship, a written agreement has to be concluded with any External Joint-Controllers (located within or outside of the EEA) stipulating that they shall, in a transparent manner, determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the Data Subject (see paragraph 4.2) and their respective duties to provide the information to said Data Subject, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the Controllers are determined by the European Union or Member State law to which the Controllers are subject. Data Protection contacts (e.g. Local CRM managers) and appointed data protection officers, in coordination with the Global CRM Manager, the Global Privacy Office, shall be able to provide templates of the appropriate clauses to a Local Data Controller within the HERMES Group.

3. **All Transfers of Personal Data to External Processors located out of the EEA** in a country not recognized by the EU Commission as ensuring an adequate level of protection must respect the rules relating to the Processors (Articles 28 and 49 of the GDPR) in addition to the rules on transborder data flows (Articles 46 and 49 of the GDPR) (see §1 and 2 above)

4.8. TRAINING PROGRAMS

Any HERMES GROUP Employee who collects, processes or has access to Personal Data related to customers shall be provided with specific training programs in order to improve its practical skills and knowledge that relate to data protection issues, especially the BCRs:

1. BCR's and all related guidelines, procedures or policies shall be uploaded on HERMES GROUP corporate intranet and permanently accessible to every Employee.
2. Access to the BCRs and all related guidelines, procedures or policies shall be granted to every HERMES GROUP new Employee. Internal notices shall also be transmitted within the Group to raise awareness on the BCRs.
3. New Employees who collect, process or have access to Personal Data shall be required to follow a Data Protection compliance training program. Furthermore, all Employees who collect, process or have access to Personal Data shall be required to follow such a program, on a regular basis. [All Employees must pass a knowledge check (certification) following their completion of the training to confirm their knowledge and skills on privacy issues].
4. At local level, each Data Controller and/or Local CRM Manager shall feel free to enhance the Data Protection training programs described above by adding any appropriate training material.
5. Data Protection training programs shall be reviewed and approved by experienced HERMES GROUP officers, in coordination with the local data controller, the Local CRM Manager, the Global CRM Manager and the Global Privacy Office. Procedures related to Data Protection training programs shall be regularly audited (see paragraph 5.8).

4.9. AUDIT PROGRAMME

Data Protection audits shall be carried out on a regular basis (subject to more stringent local laws at least one audit every 3 years) by internal or external accredited audit teams to ensure that the BCRs and all related policies, procedures or guidelines are updated and applied :

1. Data Protection audits shall cover all aspects of the BCRs and all related policies, procedures or guidelines, including methods of insuring that corrective measures will take place. However, the scope of each audit can be strengthened to limited aspects of the BCRs and/or the related policies, procedures or guidelines, including methods of insuring that corrective measures will take place.

2. Data Protection audits shall be decided directly by the Compliance Department or upon specific request of the Head Controller, a Local Data Controller, a Local CRM Manager, the Global CRM Manager or the Global Privacy Office. The ones in charge of handling an audit will always benefit from an appropriate level of independence in the exercise of their duties.

3. The results of all audits shall be communicated to the Head Controller (especially to the ultimate parent's board), and the Local Data Controller, and/or the Local CRM Manager, and/or the Global CRM Manager, and/or the Global Privacy Office.

4. The relevant Supervisory Authorities shall receive a copy of such audit upon request. Each Local Data Controller shall accept to be audited by a Supervisory Authority and to abide by the advice of a Supervisory Authority on any issue related to the BCRs.

5. As provided by section 3 of paragraph 6.1, Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office shall report every year to the Head controller about all the actions and measures taken with regard to Data Protection issues (training programs, inventory of Personal Data Processing implemented, management of complaints, etc.). Furthermore, each local data CRM Manager shall take every necessary step to make sure that local data controllers comply with the provisions of the BCRs. To this end, a "BCR compliance check-list" shall be used at local level to make compliance checks.

6. The Global CRM Manager and the Global Privacy Office shall also regularly report to the Head Controller about the implementation of the BCRs within each local Data Controller.

7. Based on the audit results and the reports mentioned above, the Head Controller (especially to the ultimate parent's board), and/or the Global CRM Manager, and/or the Global Privacy Office shall decide any appropriate legal, technical or organizational measure in order to improve Data Protection management within the Group, both at global and/or local level.

5. BINDINGNESS OF THE BCRs

5.1. INTERNAL BINDING NATURE

The present BCRs bind all HERMES GROUP entities which have signed the BCR Intra-Group Agreement (Appendix 5) setting out and expressing their acceptance of the BCRs.

Each HERMES GROUP entity that signs the BCR Contractual Agreement Form is responsible for administering and overseeing the implementation of these BCRs, including making these BCRs binding upon the Employees who have a duty to comply with the obligations set out therein.

Pursuant to applicable local labor law, the BCRs are made binding towards the Employees either through work employment contracts or through collective agreements, through relevant company policies in which the BCRs have been incorporated or by any other means on condition that the group can properly explain how the BCRs are made binding on said Employees.

5.2. COMPLIANCE AND SUPERVISION OF COMPLIANCE

HERMES GROUP has established a data protection network composed of data protection officers (when legally required according to article 37) and/or data protection contacts appointed at global and local levels.

At local level, each appointed data protection officer (DPO) and Local CRM Manager shall be responsible for the implementation of the BCRs. Thus:

1. The appointed DPO and Local CRM Manager shall inform and advise the Local Data Controllers and the Employees who carry out Processing on their obligations;

2. Each entity of the HERMES GROUP shall take every necessary step to make sure that Local Data Controllers comply with the provisions of the BCRs. To this end, a "BCR compliance check list" shall be used at local level to make compliance checks. Data Protection audits decided by the Compliance Department, the Global CRM Manager or the Global Privacy Office may focus on how these compliance checks are made at local level.

3. DPO, Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall always be at the disposal of both Local Data Controller and Data Subjects to provide any help with regard to a data protection issue, especially the BCRs.

4. DPO, Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall provide advice, where requested, with regard to the conduct of any data protection impact assessment and the monitoring of its performance where required.

5. DPO, Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall report every year to the Head controller about all the actions and measures taken with regard to data protection issues (training programs, inventory of Personal Data Processing implemented, management of complaints, etc.), especially the implementation of the BCRs.

6. Each Local Data Controller, DPO and Local CRM Manager shall regularly report to the Global CRM Manager and the Global Privacy Office about the complaints settled at local level, with a view to take corrective actions and improve guidelines and procedures implemented within the Group, where the complaints may have revealed a "gap" in terms of Data Protection.

7. DPO, Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall be able to provide any appropriate templates (i.e. notices of information, clauses, etc.) to each Local Data Controller within the Group for any purpose related to a data protection issue.

8. DPO, Local CRM Managers, in coordination with the Global CRM Manager and the Global Privacy Office, shall cooperate with the Supervisory Authorities and act as the contact point for the Supervisory Authorities on issues relating to Processing.

Furthermore, in terms of supervision of compliance, specific measures shall be taken to ensure the right implementation of the BCRs:

1. The Global CRM Manager and the Global Privacy Office shall regularly report to the Head Controller about the implementation of the BCRs within each Local Data Controller and within each Processor that is a member of the HERMES GROUP.

2. Data protection audits shall be decided directly by the Compliance Department or upon specific request of a Local Data Controller, a DPO, a Local CRM Manager, the Global CRM Manager or the Global Privacy Office. The results of all audits or reports shall be communicated to the Head Controller (especially to the ultimate parent's board), and the Local Data Controller and/or the DPO, and/or the Local CRM Manager, and/or the Global CRM Manager, and/or the Global Privacy Office.

3. Based on the audit results and the reports mentioned above, the Head Controller (especially Head Controller's management), the Global CRM Manager, the Global Privacy Office, a Local Data Controller or a DPO or a local CRM Manager shall decide any appropriate measure in order to improve Data Protection management within the Group, both at global and/or local level.

4. If a violation of the BCRs is established, any correction measure (legal, technical or organizational measure) as well as any appropriate sanction (against the local Data Controller or, according to local labor law, a local Employee) may be taken on the initiative of the Head Controller, the Global CRM Manager, the Global Privacy Office, a Local Data Controller or a DPO or a Local CRM Manager.

5. Data Protection training programs shall be reviewed and approved by HERMES GROUP senior officers, in coordination with the Global CRM Manager, the Global Privacy Office, the DPO and Local CRM managers. Procedures related to Data Protection training programs shall be regularly audited (see paragraph 4.9).

6. The Global CRM Manager, the Global Privacy Office and DPO will liaise with the Lead Supervisory Authority pursuant to Article 56 of the GDPR.

5.3. THIRD PARTY BENEFICIARY RIGHTS

1. A Data Subject who claims to have suffered damage as a direct result of a violation of the provisions of the BCRs listed below and/or Appendix 2 of these BCRs, and who either is not satisfied with the resolution of their complaint, as described in paragraph 4.4, or desires to bypass the internal complaint mechanism and bring their complaint directly to the relevant Supervisory Authority, may seek to enforce their third party beneficiary rights before the relevant Supervisory Authority or at the courts according to the principles and terms as set out below. The complaint handling procedure shall support Data Subjects' ability to address any data protection complaint internally. Data Subjects are however free to lodge a complaint directly with the Supervisory Authority or the courts as provided by local laws.

2. A Data Subject shall have the right to enforce, as a third party beneficiary, the provisions of the BCRs related to:

- Purpose limitation(see paragraph 2.2 and appendix 2)
- Data quality and data minimization (see paragraph 2.2 and Appendix 2)
- Lawfulness principles for Processing Personal Data and Special Categories of Data (see paragraph 2.2 and Appendix 2)
- Fairness and Transparency principle, right of information, and easy access to BCRs (see paragraphs 2.2 and .1 and Appendix 2)
- Rights of access, rectification, erasure, restriction of Processing, objection to Processing and right to data portability (see paragraph .2)
- Rights in case of Automated Individual Decision Making (including Profiling) are taken (see paragraph .3)
- Security and confidentiality principles (see paragraph 4.5)
- Restrictions on onward Transfers outside of the group of companies (see paragraph 4.7.)
- National legislation preventing respect of BCR (see paragraph 6.2.)
- Right to complain through the internal complaint mechanism (see paragraph 4.4.)
- Cooperation duties with Supervisory Authority (see paragraph 5.6)
- Liability and jurisdiction provisions (see paragraphs 4.4. and 5.4)

As a rule regarding jurisdiction for any claim, each Data Subject shall have the right to take its case, at its best convenience, to the competent Supervisory Authorities (where the GDPR is applicable, in the EU Member State of his habitual residence, place of work or place of the alleged infringement) or before the jurisdiction of the Local Data Exporter or before the jurisdiction of the Local Data Importer (where the GDPR is applicable, the court of the EU Member State where the Local Data Controller or Processor has an establishment or where the Data Subject has his habitual residence).

3. According to the relevant provisions in paragraph 4.3.1, each Data Subject who has suffered damage shall be entitled to receive compensation as may be ordered by the appropriate court or regulatory agency (e.g., judicial remedies) or as decided according to the internal complaint mechanism, if used.

4. The BCRs shall always be readily available to every Data Subject, in the conditions described in paragraph 4.1.

5. HERMES GROUP entities bound by the BCRs shall abide by a decision of a competent court or a competent Supervisory Authority (provided such court is a court of the EU Member State where the Local Data Controller or Processor has an establishment or where the Data Subject has his habitual residence or such authority is located in the EU Member State of the habitual residence, place of work of the Data Subject or place of the alleged infringement) which is final and against which no further appeal is possible.

5.4. LIABILITY

Each HERMES GROUP entity located within the EU which violates the BCRs and causes damages to Data Subjects shall be liable and shall take the necessary remedial actions unless the HERMES GROUP entity concerned can demonstrate that such damages cannot be attributed to it and its providers for any breach of the BCRs.

HERMES INTERNATIONAL accepts responsibility for and agrees to take the necessary actions to remedy the acts of other HERMES GROUP entities located outside the EU and to pay compensation for any material and non-material damages resulting from the violation of the BCR by such HERMES GROUP entities, unless HERMES INTERNATIONAL can demonstrate that such damages cannot be attributed to a HERMES GROUP entity located outside the EU or to its providers.

If a HERMES GROUP entity located outside of the EU violates the BCR, the courts and other competent authorities in the EU will have jurisdiction and the Data Subjects will have the rights and remedies against HERMES INTERNATIONAL as if the violation has been caused by that HERMES GROUP entity.

HERMES INTERNATIONAL reserves the rights to pursue remedies against the HERMES GROUP entities located outside the EU which violated the BCR.

All HERMES GROUP entities shall have sufficient financial resources at their disposal to cover the payment of compensation for breach of the BCR. Liability as between the parties shall be limited to actual damage suffered. Indirect (i.e., consequential damages such as reputational damages) or punitive damages (i.e., damages intended to punish a party for its outrageous conduct) shall be explicitly excluded.

The above liabilities shall not be affected by any action HERMES GROUP may take against its providers or other third parties potentially involved in the Processing of information.

5.5. SANCTIONS

Would a violation of the BCRs, either by Local Data Controller representatives or Employees, be established, any appropriate disciplinary sanction or judicial action may occur, in accordance with local labor law, on the initiative of the Head Controller, the Global CRM Manager, the Global Privacy Office, the Local Data Controller or the DPO or the Local CRM Manager.

Thus, each Local Data Controller, DPO and Local CRM Manager shall pay specific attention to any audit results (see paragraph 5.8) establishing non-compliance issues against representatives or Employees, especially in case of non-compliance with the Data Protection Principles and the applicable guidelines, procedures and policies related to the implementation of the BCRs.

5.6. MUTUAL ASSISTANCE AND COOPERATION WITH SUPERVISORY AUTHORITIES

All HERMES GROUP entities bound by the BCR are committed to a full cooperation with the EEA Supervisory Authorities who have competent jurisdiction. Thus:

- The relevant Supervisory Authorities shall receive, upon request and within a reasonable time frame, an updated copy of the BCRs or all related procedures, policies or guidelines.
- The Local Data Controller shall reply within a reasonable period of time to any request addressed by a relevant Supervisory Authority with competent jurisdiction, to their requests concerning the interpretation and application of the BCRs.

- The Local Data Controller shall apply any relevant recommendation or advice from a relevant Supervisory Authority relating to the implementation of the BCRs.
- HERMES GROUP entities bound by the BCRs commit to accepting audits from the competent EEA Supervisory Authorities
- The Local Data Controller shall abide by a decision of a relevant Supervisory Authority with competent jurisdiction, related to the implementation of the BCRs, against which no further appeal is possible before competent courts.
- The Global CRM Manager and the Global Privacy Office and DPO shall be at the disposal of the relevant Supervisory Authorities for any matter related to the implementation of the BCRs.

Furthermore, members of HERMES GROUP shall cooperate and assist each other to handle a request or complaint from an individual (see paragraph .4) or inquiry by Supervisory Authorities.

6. FINAL PROVISIONS

6.1. RELATIONSHIP BETWEEN NATIONAL LAWS AND THE BCRs

HERMES GROUP undertakes that appropriate entities and Employees of the HERMES GROUP shall comply with the provisions of the BCRs, as well as with the provision of the GDPR and 2002/58 EU Directive and applicable local laws.

Where the local legislation requires a higher level of protection for Personal Data, it always will take precedence over the BCRs. When in doubt, the concerned HERMES GROUP entities may consult the competent Supervisory Authorities and/or the Lead Supervisory Authority.

6.2. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT OF BCRs

Shall a Local Data Controller have reasons to believe that the legislation applicable to Local Data Controller prevents Local Data Controller from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided by the BCRs, the Local Data Controller will promptly inform the Global CRM Manager or the Global Privacy Office (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Where there shall be conflict between national law and the commitments in the BCRs, the DPO, the Local CRM Manager and the local Data Controller, in coordination with the Global CRM Manager and the Global Privacy Office, consult the competent Supervisory Authorities in case of doubt and are responsible for making a decision regarding the conflict.

In addition, where any legal requirement a Local Data Controller is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the BCR, the problem should be reported to the competent Supervisory Authorities. This includes any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body. In such a case, the competent Supervisory Authorities should be clearly informed about the request, including information about the Personal Data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

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

If, in the above cases, despite having used its best efforts, the requested Local Data Controller is not in a position to notify the competent Supervisory Authorities, this Controller commits to annually providing general information on the requests it received to the competent Supervisory Authorities (e.g. number of applications for disclosure, type of Personal Data requested, requester if possible, etc.).

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

6.3. UPDATES OF THE BCRs

In case of, for instance, changes in laws or HERMES GROUP procedures, the terms of the BCRs may be updated on the initiative of the Head Controller, in coordination with the Global CRM Manager and the Global Privacy Office.

Global CRM ManagerGlobal CRM Manager

Any modification of the BCR has to be reported by HERMES GROUP without undue delay to all HERMES GROUP entities members of the BCR and to the relevant Supervisory Authorities via the Lead Supervisory Authority.

In addition, updates of the BCRs or to the list of the HERMES GROUP entities members of the BCRs are possible without to re-apply for an approval as HERMES GROUP undertakes the following:

- The Global CRM Manager and the Global Privacy Office keep an updated list of the HERMES GROUP entities members and keep track of and record any updates to the rules;

- HERMES GROUP will provide the necessary information about any updates to the rules to the Data Subjects and to any other relevant Data Protection Authorities upon request.
- No Transfer shall be made to a new HERMES GROUP entity until this new entity is effectively bound by the BCR and can deliver compliance.
- Any change to the BCRs or to the list of HERMES GROUP entities members will be reported once a year to the Lead Authority;
- Any changes which would affect the level of protection offered by the BCRs or will significantly affect the BCRs (i.e., changes to the bindingness character) will be communicated to the relevant Supervisory Authorities via the Lead Supervisory Authority.

6.4. APPLICABLE LAW / JURISDICTION / TERMINATION / INTERPRETATION OF TERMS

The BCRs shall be adopted by the Head Controller, in coordination with the Global CRM Manager and the Global Privacy Office.

The BCRs shall take effect on the date when each entity of the HERMES GROUP signs this BCRs agreement and, as a consequence, is legally bound.

Each entity of the HERMES GROUP recognizes to be bound by the BCRs, from the date of signature of the BCRs agreement and without any other formalities, with respect to other HERMES GROUP entities already bound or about to be bound from the date of their signature, notwithstanding the date and place of signature of a BCRs agreement by each other entity of the HERMES GROUP involved, and provided that the terms of the BCRs are strictly identical between each other. Except if an entity of the HERMES GROUP is able to prove that the signed BCRs agreement is not strictly identical to the ones signed by other entities, it expressly and irrevocably disclaims challenging the evidence that it is bound by the terms of the BCRs.

In the event that a Local Data Exporter or a Local Data Importer would be found in substantial or persistent breach of the terms of the BCRs, the Head Controller may temporarily suspend the Transfer of Personal Data until the breach is repaired. Should the breach not be repaired in due time, the Head Controller shall take the initiative to terminate the BCRs Agreement with respect to that specific Local Data Exporter or Local Data Importer. In such a case, the Local Data Exporter or Local Data Importer shall take every necessary step in order to respect the European rules on transborder data flows (Article 46 of the GDPR) for instance by making use of the EU Standard Contractual Clauses approved by the EU Commission.

The provisions of the BCRs shall be governed by Applicable Data Protection Law. Jurisdiction shall be attributed to the courts of the Local Data Importer or Local Data Exporter

In case of contradiction between the BCRs and the appendixes, the main body of the BCRs shall always prevail. In case of contradiction between the BCRs and other global or local policies, procedures or guidelines, the BCR shall always prevail. In case of contradiction or inconsistency, the terms of the BCRs shall always be interpreted and governed by the provisions of the GDPR and 2002/58 EU Directives.

[To be signed by each legal entity of the HERMES GROUP bound by the BCRs according to the contractual agreement form set out in appendix 5]

APPENDICES

- Appendix 1 – Definitions
- Appendix 2 – Data Protection Principles
- Appendix 3 – List of HERMES GROUP entities bound by the BCRs
- Appendix 4 – Nature and purposes of the Personal Data being transferred within the scope of the BCRs
- Appendix 5 – Contractual agreement form

APPENDIX 1: DEFINITIONS

The terms and expressions used in the BCRs are defined in this appendix, provided that these terms and expressions shall always be interpreted according to the EU 95/46 and 2002/58 Directives.

"**Applicable Data Protection Law**" shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data applicable to a Data Controller located in any country where HERMES GROUP is located and in which the Local Data Exporter is established.

"**Automated Individual Decision Making**" shall mean a decision which produces legal effects or significantly affects a Data Subject and which is based solely on automated Processing of Personal Data in order to evaluate this person.

"Consent" of a Data Subject means any freely given, specific, informed and unambiguous indication, through a statement or clear affirmative action, of the Data Subject's agreement to the Processing of his or her Personal Data.

"**Data Subject**" shall mean an identified or identifiable person to whom specific Personal Data relates. It is someone who can be identified, directly or indirectly, in particular by reference 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.

"**Data Transfer**" shall mean any transfer of Personal Data from an entity to another entity. A transfer can be carried out via any communication, copy, transfer or disclosure of Personal Data through a network, including remote access to a database or transfer from a medium to another, whatever the type of medium (for instance from a computer hard disk to a server).

"**EEA or European Economic Area**" shall mean the countries of the European Union and member countries of EFTA (European Free Trade Association).

"Employee(s)" shall mean the person or alternatively any people who perform, or have in the past performed, duties for the HERMES GROUP, in exchange for wages or a salary, under an employment contract (where applicable or required by law) or any other assimilated agreement (such as internship agreement) and under a subordination relationship. This also includes directors, trainees, apprentices, contingent workers and assimilated status.

"General Data Protection Regulation" (or "GDPR") means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing directive 95/46/EC.

"**Global CRM Manager**" shall mean the senior level manager who is responsible, within the Group at Global level, for managing business awareness and adequation with Applicable Data Protection Law and HERMES GROUP privacy policies, procedures and guidelines, especially the BCRs.

"**Global Privacy Office**" shall mean the department located within the Head Controller Offices who is in charge, within the Group at worldwide level, for managing business awareness and compliance with Applicable Data Protection Law and HERMES GROUP data protection policies, procedures and guidelines, especially the BCRs.

"**Hermes Group**" shall mean HERMES INTERNATIONAL itself and/or any corporate entity of the HERMES GROUP hold, directly or indirectly, by HERMES INTERNATIONAL, according to article L. 233-3 of the French Commercial Code.

"**Head Controller**" shall mean HERMES GROUP Headquarters located in France which alone or jointly with others determines the purposes and means of the Processing of Personal Data and which is in charge of the formal adoption of BCRs to be implemented within HERMES GROUP.

"Joint-Controller" shall mean two or more Controllers which jointly determine the purpose(s) and the means of the Processing.

"**Lead Supervisory Authority**" shall mean the French Supervisory Authority ("CNIL").

"**Local Data Controller**" shall mean the legal entity of the HERMES GROUP which alone or jointly with others determines the purposes and means of the Processing of Personal Data; where the purposes and means of Processing are determined by national or EU laws or regulations, the controller or the specific criteria for his nomination may be designated by national or EU law.

"**Local Data Exporter**" shall mean the legal entity of the HERMES GROUP located within the EEA which transfers the Personal Data outside the EEA.

"**Local Data Importer**" shall mean the legal entity of the HERMES GROUP located outside the EEA which agrees to receive from the Local Data Exporter Personal Data for further Processing.

"**Local CRM Manager**" shall mean an experienced HERMES GROUP officer within a Local Data Controller who is responsible for managing business awareness and adequation with applicable data protection law and HERMES GROUP data protection policies, procedures and guidelines, especially the BCRs.

"**Personal Data**": shall mean any information relating to an identified or identifiable natural person ("Data Subject").

"**Personal Data Concerning Health**" means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data that has been transmitted, stored or otherwise processed.

"**Processing of Personal Data**" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processor**" shall mean a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the controller.

"Profiling" means 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.

"Pseudonymisation" means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to Technical and Organizational Measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

"**Recipient**" shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a Third Party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as Recipients.

"**Records of Processing Activities**" shall mean the records of all of the information set forth in Article 30 of the GDPR which each Controller or his representative and each Processor shall maintain with regard to all Processing activities under his responsibility.

"**Special Categories of Personal Data**" shall mean Personal Data revealing directly or indirectly the racial or ethnic origin, political opinions, philosophical or religious beliefs, trade union affiliation, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, or data related to the health or sexual life of individuals.

"**Supervisory Authority**" shall mean an independent body which is in charge of: (i) monitoring the Processing of Personal Data within its jurisdiction (country, region or international organization), (ii) providing advice to the competent bodies with regard to legislative and administrative measures relating to the Processing of Personal Data, and (iii) hearing complaints lodged by citizens with regard to the protection of their data protection rights.

"**Third Party**" shall mean any 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.

"**Technical and organizational security measures**" shall mean measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing. **"2002/58 EU Directive"** shall mean Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the protection of privacy in the electronic communications sector (as amended).

APPENDIX 2: DATA PROTECTION PRINCIPLES

Within the scope of the BCRs, any Transfer of Personal Data to a third country which does not ensure an adequate level of protection shall always comply with the following data protection principles, set out by the GDPR.

FAIRNESS & TRANSPARENCY

Fairness requires that the Data Subject be informed of the existence of the Processing operation and its purposes.

Any information and communication relating to the Processing of the Data Subjects' Personal Data shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. That principle concerns, in particular, information to the Data Subjects on the identity of the controller and the purposes of the Processing and further information to ensure fair and transparent Processing in respect of the natural persons concerned and their right to obtain confirmation and communication of Personal Data concerning them which are being processed.

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.

LAWFULNESS OF PROCESSING OF PERSONAL DATA

Personal data shall be processed only if:

- the Data Subject has given his Consent to the Processing of his or her Personal Data for one or more specific purposes;
- the 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;
- the Processing is necessary for compliance with a legal obligation to which the Controller is subject;
- the Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- the 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;
- the Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by the Third Party or Parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

LAWFULNESS OF PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

Special Categories of Personal data, especially Personal Data Concerning Health, shall be processed only if:

- the data subject has given his explicit Consent to such Processing for one or more specified purposes, except where the applicable laws prohibit it;
- the Processing is necessary for the purposes of carrying out the obligations and specific rights of the Controller and the Data Subject in the field of employment law and social security and social protection in so far as it is authorized by European Union or national law or a collective agreement providing for adequate safeguards for the fundamental rights and the interests of the Data Subjects;
- the Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent;
- the Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking 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 data is not disclosed outside the body without the Consent of the Data Subjects ;
- the Processing relates to Special Categories of Personal Data which is manifestly made public by the Data Subject;
- the Processing of Special Categories of Personal Data is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- the Processing of the Special Categories of Personal Data is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Employee, for medical diagnosis, the provision of health or social care or treatment or the management of health-care or social-care systems and services, on the basis of national law or pursuant to a contract with a health professional and subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Other special categories of data (such as mainly criminal data) may be subject to local data protection requirements provided by national law. In particular, Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or when the Processing is authorized by national law providing appropriate safeguards for the rights and freedoms of Data Subjects.

In addition, national law may further determine the specific conditions for the Processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the Data Subject pursuant to the national law.

PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

Further Processing of data for archiving purposes, in the public interest, scientific or historical research purposes or statistical purposes shall not be considered as incompatible provided that appropriate safeguards for the rights and freedoms of the Data Subjects - and in particular Technical and Organizational Measures - are implemented in order to ensure data minimization.

DATA MINIMIZATION, LIMITED STORAGE PERIODS AND DATA QUALITY

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or further processed (Data minimization);

Personal data shall be accurate and, where necessary, kept up to date (accuracy). Every reasonable step shall 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.

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Personal Data may be stored for longer periods as long as it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate Technical and Organizational Measures in order to safeguard the rights and freedoms of the Data Subject (limited storage periods).

DATA PROTECTION BY DESIGN AND BY DEFAULT:

Data protection by design: the Local Data Controller must implement, both at the time of the determination of the means for Processing and at the time of the Processing itself, appropriate Technical and Organizational Measures (such as Pseudonymization) designed to implement data protection principles (such as data minimization), in an effective manner and to integrate the necessary safeguards into the Processing.

Data protection by default: the Local Data Controller must implement appropriate Technical and Organizational Measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed.

SECURITY OF PERSONAL DATA

Appropriate technical and organizational measures shall be implemented to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to and against all other unlawful forms of Processing (see paragraph 4.5).

ONWARD TRANSFERS TO ORGANIZATIONS NOT BOUND BY BCRS

When Personal Data is intended to be transferred to a non-HERMES GROUP entity, adequate safeguards have to be implemented (see paragraph 4.7).

ACCOUNTABILITY

The Local Data Controller shall be responsible for, and be able to demonstrate compliance with the present data protection principles (accountability).

In order to demonstrate compliance, BCR members need to maintain a Record of Processing Activities carried out in line with the requirements as set out in Article 30 of the GDPR. Where appropriate, the Local Data Controller must implement appropriate data protection policies.

In order to enhance compliance and when required, data protection impact assessments should be carried out for Processing operations that are likely to result in a high risk to the rights and freedoms of natural persons (Article 35 of the GDPR). Where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Local Data Controller to mitigate the risk, the competent Supervisory Authority, prior to the Processing, should be consulted (Article 36 of the GDPR).

APPENDIX 3: LIST AND LOCATION OF HERMES GROUP ENTITIES BOUND BY THE BCRs

1. HERMES GROUP entities located within the EEA

HEAD CONTROLLER

France:

HEAD CONTROLLER	HERMES INTERNATIONAL
Form	Société en commandite par actions
Registered address	24, rue du Faubourg Saint-Honoré 75008 Paris (France)
TVA communautaire	FR
Legal representative	Axel DUMAS
Global CRM Manager	Bénédicte REVOL
Global Privacy Office	Legal Department - DPO
Local CRM Manager	Armelle Laurent

LOCAL DATA CONTROLLER

France:

LOCAL DATA CONTROLLER	COMPAGNIE DES ARTS DE LA TABLE ET DE L'EMAIL (LA TABLE HERMES)
Form	Société par actions simplifiée à associé unique
Registered address	Route de Piégut 24300 Nontron (France)

LOCAL DATA CONTROLLER	COMPTOIR NOUVEAU DE LA PARFUMERIE (HERMES PARFUMS)
Form	Société anonyme
Registered address	23, rue Boissy d'Anglas 75008 Paris (France)

LOCAL DATA CONTROLLER	COMPAGNIE DES CRISTALLERIES DE SAINT-LOUIS
Form	Société par actions simplifiée
Registered address	57620 Saint-Louis-lès-Bitche (France)

LOCAL DATA CONTROLLER	CREATIONS METAPHORES
Form	Société par actions simplifiée
Registered address	21, rue Cambon 75001 Paris (France)

LOCAL DATA CONTROLLER	HERMES SELLIER
Form	Société par actions simplifiée
Registered address	24, rue du Faubourg Saint-Honoré 75008 Paris

LOCAL DATA CONTROLLER	PUIFORCAT
Form	Société par actions simplifiée à associé unique
Registered address	48 AV GABRIEL 75008 PARIS

LOCAL DATA CONTROLLER	John Lobb
Form	Société par actions simplifiée
Registered address	23 RUE BOISSY D'ANGLAS 75008 PARIS

Belgium / Luxemburg:

LOCAL DATA CONTROLLER	HERMES BENELUX NORDICS
Form	Société anonyme de droit belge
Registered address	50, Boulevard de Waterloo, 1000 Bruxelles

Denmark :

LOCAL DATA CONTROLLER	HERMES DENMARK
Form	Anpartsselskab (ApS)
Registered address	c/o NJORD Law Firm, Pilestrade 58, 1112 Copenhagen K

Germany:

LOCAL DATA CONTROLLER	HERMES GmbH
Form	Société à responsabilité limitée de droit allemand
Registered address	Marstallstrasse 8, 80539 Munich

United Kingdom:

LOCAL DATA CONTROLLER	HERMES GB Ltd
Form	Société à responsabilité limitée de droit anglais
Registered address	1 Bruton Street W1J 6TL London

LOCAL DATA CONTROLLER	**JL & Co. Ltd - *(John Lobb)***
Form	Limited Liability Company
Registered address	Westminster Works, 1 Oliver Street Northampton NN2 7JL England

Spain:

LOCAL DATA CONTROLLER	HERMES IBERICA
Form	Société anonyme de droit espagnol
Registered address	Calle Ortega y Gasset 28006 Madrid

Sweden:

LOCAL DATA CONTROLLER	HERMES SWEDEN AB

Form	AB (Private Limited Company)
Registered address	NK 243, 111 77 Stockholm

Italy:

LOCAL DATA CONTROLLER	HERMES Italie SPA
Form	Société anonyme de droit italien
Registered address	Via Serbelloni 1, 20122 Milan

Greece:

LOCAL DATA CONTROLLER	HERMES GRECE
Form	Société anonyme de droit grec
Registered address	Rue Stadiou 4 et Rue Voukourestiou 1, 10564 Athènes

Czech Republic:

LOCAL DATA CONTROLLER	HERMES PRAGUE
Form	Société anonyme de droit tchèque
Registered address	Parizka 12 :120, 110000 Prague

Portugal:

LOCAL DATA CONTROLLER	HERMES INTERNATIONAL PORTUGAL
Form	Société de droit portugais
Registered address	Largo do Chiado 9, 1200-108 Lisbonne

Poland:

LOCAL DATA CONTROLLER	HERMES POLOGNE SP. Z O.O
Form	limited liability company
Registered address	ul. Krakowskie Przedmieście 13 00-071 Warszawa

2. HERMES GROUP entities located outside the EEA

Turkey:

LOCAL DATA CONTROLLER	HERMES ISTANBUL
Form	
Registered address	Abdi Ipekçi Cad N°79 Nisantasi Sisli Istanbul

Monaco:

LOCAL DATA CONTROLLER	HERMES MONTE CARLO
Form	Société Anonyme de droit monégasque

Registered address	11.13.15 avenue de Monte-Carlo 98000 Monaco (Principauté de Monaco)

Russia:

LOCAL DATA CONTROLLER	HERMES RUS
Form	SARL
Registered address	Nizhniy Kiselny Pereulok 4, 107 031 MOSCOW

Switzerland:

LOCAL DATA CONTROLLER	HERMES (SUISSE)
Form	Société Anonyme de droit Suisse
Registered address	4, rue de la Tour de l'Ile 1204 Genève

ZONE AMERIQUES

United States :

LOCAL DATA CONTROLLER	CREATIONS METAPHORES
Form	Société anonyme de droit américain
Registered address	55 east 59th Street – NYC 10022 - USA

LOCAL DATA CONTROLLER	HERMES OF PARIS Inc
Form	Société anonyme de droit américain
Registered address	55 East 59th Street – NYC 10022 - USA

Canada:

LOCAL DATA CONTROLLER	HERMES CANADA INC
Form	Société de droit canadien
Registered address	130 Bloor Street West, Toronto, Ontario M5S 1N5 (Canada)

Mexico:

LOCAL DATA CONTROLLER	BOISSY MEXICO
Form	
Registered address	Avenida Presidente Mazaryk 422, Local A Col Polanco, 11560 Mexico DF (Mexique)

Argentina:

LOCAL DATA CONTROLLER	HERMES ARGENTINA
Form	Sarl de droit argentin
Registered address	Avenida Alvear 1981 – 1129 Buenos Aires (Argentine)

Brazil:

LOCAL DATA CONTROLLER	H BRASIL COMERCIO IMPORTACAO E EXPORTACAO Ltda
Form	L.T.D.A
Registered address	Avenida Magalhaes de Castro, n°12.000 Loja 32, Piso Terreo, Jardim Panarama, CEP 05502-001, Sao Paulo, Brazil

ZONE ASIA - PACIFIC

Singapore:

LOCAL DATA CONTROLLER	HERMES MIDDLE EAST SOUTH ASIA
Form	Private Limited Company
Registered address	1 Marina Bld 2800/018989 Singapour

LOCAL DATA CONTROLLER	HERMES SOUTH EAST ASIA (HSEA)
Form	Ltd
Registered address	1 Marina Bld 2800/018989 Singapour

LOCAL DATA CONTROLLER	HERMES SINGAPORE RETAIL
Form	Private Limited Company
Registered address	1 Marina Bld #2800/018989 Singapour

LOCAL DATA CONTROLLER	BOISSY SINGAPOUR (TR Singapore)
Form	Private Limited Company
Registered address	One Marina Boulevard #28-00 Singapour 018989 (Singapour)

Hong-Kong:

LOCAL DATA CONTROLLER	HERMES ASIA PACIFIC
Form	Ltd
Registered address	25F, Chinachem Leighton Plaza, 29 Leighton Road – Causeway Bay – Hong-Kong (RPC)

LOCAL DATA CONTROLLER	HERLEE LIMITED (TR HK)
Form	Ltd
Registered address	25/F Chinachem Leighton Plaza, 29 Leighton Road, Causeway Bay, Hong Kong

China:

LOCAL DATA CONTROLLER	HERMES (CHINA) CO LTD
Form	Ltd
Registered address	Room 3010, 3011 – Westgate Mall Tower

	1038 Nanjing Xi Road, Shanghai 2000141 (Chine)

LOCAL DATA CONTROLLER	HERMES (CHINA) TRADING CO. LTD
Form	Ltd
Registered address	Building N°12, N° 211, 213, 215 et 227 Middle Huaihai Road, Shanghai PRC

LOCAL DATA CONTROLLER	SHANG-XIA
Form	A Chinese company
Registered address	233, Huaihai Middle Road, Shanghai, 200021, PRC

Thailand:

LOCAL DATA CONTROLLER	SAINT HONORE BANGKOK
Form	Ltd
Registered address	2 Sukhumvit Road, Kwaeng Klagton Khet Kiongtoey – Bangkok – Thaïlande

Malaysia:

LOCAL DATA CONTROLLER	HERMES RETAIL (MALAYSIA)
Form	Private Limited Company
Registered address	Level 16, Memara TM Asia Life, 189 Jalan Inn Razan 50400 Kuala Lumpur (Malaisie)

India:

LOCAL DATA CONTROLLER	HERMES INDIA RETAIL AND DISTRIBUTORS
Form	Private Limited Company de droit indien
Registered address	G/5 – Shopping Arcade, The Oberoi – Dr Zakir Hussain Marg. 110003 New Delhi (Inde)

Japan:

LOCAL DATA CONTROLLER	HERMES JAPON CO LTD
Form	Kabushiki Kaisha
Registered address	4-3 Ginza 5-Chome Chuo-Ku Tokyo 104-0061 (Japon)

Australia:

LOCAL DATA CONTROLLER	HERMES AUSTRALIA PTY LTD
Form	Ltd
Registered address	Level 11, 70 Castlereagh Street NSW 2000 Sydney (Australie)

Taiwan:

LOCAL DATA CONTROLLER	HERMES ASIA PACIFIC -TAIWAN
Form	Ltd
Registered address	Basement 1st Floor, n°3, Lane 39, Sec 2, Chang-Chan North Road TAIPEI

South Korea:

LOCAL DATA CONTROLLER	HERMES KOREA LIMITED
Form	Ltd
Registered address	630-26, Shinsa-Dong Gangnam-gu, 135-895 SEOUL

Guam:

LOCAL DATA CONTROLLER	Faubourg Guam Inc (TR Guam)
Form	Inc
Registered address	Suite 331, Tumon Sands Plaza, 1082 Pale San Vitores Road, Tumon, Guam 96913

Saipan:

LOCAL DATA CONTROLLER	Boissy Singapore Pte Ltd , Saipan Branch
Form	
Registered address	Suite 331, Tumon Sands Plaza, 1082 Pale San Vitores Road, Tumon, Guam 96913

APPENDIX 4: NATURE AND PURPOSES OF PERSONAL DATA BEING TRANFERRED WITHIN THE SCOPE OF THE BCRs

Purposes	Nature of the data transferred	Recipients in third countries
► Customer relationship management (CRM) i.e.: - providing customers with the products and/or services requested (including processing their payment); - conducting checks to identify customers and verify their identity; - sending marketing communications with customers' prior consent; - providing after-sale services; - responding to customers' queries, requests and suggestions; - managing the events customers are registered and/or participated in; - detecting, preventing and fighting against any fraudulent or illegal activity, including to protect customers transactions from payment fraud, to act against counterfeiting and against the resale of Hermès products in violation of Hermès terms and conditions of sale and outside of its distribution network; - managing the stock of certain types of rare products to allow a fair allocation of the products sold; - conducting statistical analysis, market research, customer satisfaction and quality assurance surveys; - improving our products and services; - providing information to regulatory bodies when legally required; - administering general record keeping.	► *Identity & contact information (including name, surname, gender, home contact details, phone number, business title, date and place of birth, email address, etc.);* ► *Goods and/or services purchased (including location of the purchase, special requests made, observations about service/products preferences, etc.);* ► *Billing details (amount of purchase, type of payment, credit/debit card details, etc.);* ► *Any information provided regarding marketing preferences or in the course of participating in surveys or promotional offers or related to a customer's request (including comments or other communications).*	► *CRM departments and departments in charge of customer relationship, retail, e-commerce, communication, legal and internal audit.*

APPENDIX 5: CONTRACTUAL AGREEMENT FORM

HERMES INTERNATIONAL

Binding Corporate Rules (BCRs) for intra-group Transfers of personal data to non-EEA countries

to be completed

The following entity of the HERMES group:

undertakes to comply with the provisions of the BCRs of the HERMES Group.

This undertaking will be relevant for:

the version dated to be completed

and for any updated BCRs that would have been notified by the HEAD CONTROLLER and/or the Global CRM Manager and/or the Global Privacy Office, 30 days prior the effective date of such new BCRs and according to articles 6.3 and 6.4 of the BCRs

On: _____ (date)

At: _____ (place of signature)

For
Name:
Surname:
Quality: