UPS - Extract – Binding Corporate Rules for Customer Personal Data

Table of Content

I. Introduction

UPS is committed to strive to conduct its business in accordance with high ethical standards and applicable laws and UPS policies, including with respect to the protection of Customer Personal Data (incl. the Personal Data of UPS Customers, Suppliers, Business Partners, and any other individual, jointly referred to as "**Customers**"). This Extract of UPS's Binding Corporate Rules for Customer Personal Data (BCRs) explains how UPS will protect the Personal Data of its Customers as defined in **Annex 1** (Definitions) to this Summary.

The BCRs entered into force on December 14, 2023 and the most recent version of the BCRs can be made available to Customers upon request. Any changes to the BCRs require the prior approval of the UPS Global Privacy Officer and must be communicated to the Group Companies without undue delay.

Any questions concerning the BCRs can be directed to the UPS Global Privacy Office:

UPS Europe SRL
Avenue Ariane 5
Brussels, B-1200
Belgium
e-mail: globalprivacy@ups.com

Capitalized terms have the meaning set out in **Annex 1** (Definitions).

II. Scope

The BCRs apply to the Processing by UPS as a Controller of Customer Personal Data originating from the EEA, that are subject to Personal Data transfer restrictions under the GDPR and that are imported and processed by another UPS Group Company.

The BCRs cover all types of Customer Personal Data, such as, for example, name and contact details (e.g., address, e-mail address, telephone number), credit card or other payment information; package tracking number; date and time of shipment and delivery; value, weight and contents of the package; information transferred through UPS information systems (e.g., shipment tracking); a digitized signature upon acceptance of the package; nature and quantity of products and services purchased including information about packages, their contents, the delivery of same; customs-related information; demographic information (e.g., age); and information about responses to UPS marketing activities.

III. Group Liability

The BCRs are legally binding on UPS and shall apply to and be enforced by UPS Europe SRL and its Group Companies, including Employees.

IV. Other Policies and Procedures

The BCRs supplement all UPS privacy policies, guidelines, and notices. UPS has developed and will continue to develop policies and procedures that comply with the BCRs. In case of conflict between the BCRs and UPS privacy policies, guidelines, and notices, the BCRs will prevail.

V. Conflict Between BCRs and Local Law

Nothing in the BCRs is construed to take away any rights and remedies that Customers may have under applicable law. The BCRs only provide supplemental rights and remedies to Customers. Where there is a conflict between applicable local law and the BCRs, UPS will consult with its Global Privacy Officer to determine how to comply with the BCRs and resolve the conflict. The Global Privacy Officer may seek the advice of the lead/competent SA.

VI. Data Protection Principles

1. Purposes for Processing

UPS may Process Customer Personal Data for the following business purposes (Business Purposes):

- **Business process execution, internal management and management reporting**: Processing that is necessary for activities such as logistical and postal services, including scheduling shipments, facilitating pick-up and delivery of shipments, route planning, load movement, volume processing, shipment optimization, risk management, conducting audits and investigations; finance and accounting, timecard and payroll tracking, implementing business controls, provision of central processing facilities for efficiency purposes, management reporting and analysis, implementing business controls, managing and using directories, developing, publishing and implementing UPS policies, managing mergers, acquisitions and divestitures, Archive and insurance purposes, legal or business consulting, and preventing, preparing for or engaging in dispute resolution;

- **Health, safety, security and integrity, including the safeguarding of the security and integrity of the business sector in which UPS operates**: Processing that is necessary to carry out activities such as those involving the protection of the interests of UPS, its Employees, Customers and the sector in which UPS operates, including the screening of Personal Data against publicly available government and/or law enforcement agency sanctions lists and other third-party data sources, the detecting, preventing, investigating and combating (attempted) fraud and other criminal or objectionable conduct, occupational health and safety, the protection of UPS and Employee assets, and the authentication of Customer, Supplier, or Business Partner status and access rights (such as required screening activities for access to UPS's premises or systems);

- **Compliance with law**: Processing that is necessary for the performance of a task carried out to comply with a legal obligation to which UPS is subject and the disclosure of Personal Data to government institutions and supervisory authorities, including tax and other competent authorities for the sector in which UPS operates;

- **Protecting the vital interests of Individuals**: Processing that is necessary to protect the vital interests of a Customer;

- **Assessment and acceptance of a Customer, conclusion and execution of agreements with a Customer, and the settlement of payment transactions**: Processing that is necessary in connection with the assessment and acceptance of Customers, including confirming and verifying the identity of relevant Individuals (this may involve the use of a credit reference agency or other Third Party), conducting due

diligence, and screening against publicly available government and/or law enforcement agency sanctions lists and other third-party data sources, the use of and participation in sector warning systems and/or third party verification services. This purpose also includes Processing of Customer Personal Data in connection with the execution of agreements and the settlement of payment transactions in the context of which UPS may provide Customer Personal Data to the counterparty or other parties as necessary, e.g., for verification or reconstruction purposes;

- **Development and improvement of products and/or services**: Processing that is necessary for the development and improvement of UPS products and/or services, research and development;

- **Performance of Customer services**: Processing that is necessary for the performance of services provided by UPS to Customers to support UPS products and services offered to or in use with their Customers. These services may include the maintenance, upgrade, replacement, inspection and related support activities aimed at facilitating continued and sustained use of UPS products and services;

- **Conclusion and execution of agreements with Customers, Suppliers and Business Partners**: Processing that is necessary to conclude and execute agreements with Customers (incl. Suppliers and Business Partners), including required screening activities (e.g., for access to UPS's premises or systems), procurement, purposes for which UPS Business Partners and other third parties may process Personal Data (for example, delivering targeted online advertising), handling Supplier and Business Partner inquiries, handling of financial services Customer, guarantor and customer of customer inquiries, and to record and financially settle delivered services, products and materials to and from UPS (including supply chain financing, asset-based lending, international trade finance, letters of credit, insurance solutions and insurance claims handling, business credit cards, and equipment leasing, lines of credit and other financial services); or

- **Relationship management and marketing**: Processing that is necessary to carry out activities such as maintaining and promoting contact with Customers, potential Customers, Suppliers, Business Partners and Individuals, account management, customer service, recalls, collection of Customer Personal Data through UPS websites, and the development, execution and analysis of market surveys and marketing strategies.

2. Lawfulness of the Processing

All Processing of Customer Personal Data is justified by one of the following legal grounds:

- The Processing is necessary for the performance of a contract with the Customer or in order to take steps at the request of the Customer 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 to protect the vital interests of the Customer or of another person;

- The Processing is necessary for the performance of task carried out in the public interest;

- The Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Customer;

- The Customer has given consent to the Processing for one specific purpose. If a Business Purpose does not exist or if applicable law requires it, UPS shall obtain the consent of the Customer. When seeking consent, UPS will inform the Customer about the purposes of the Processing, the Group Company that is responsible for the Processing, the right of the Customer to withdraw consent at any time without consequence to his or her employment relationship.

3. Secondary Purposes for Processing Customer Personal Data

UPS will normally only Process Customer Personal Data for the Business Purposes. However, Customer Personal Data may be Processed for a purpose other than the Business Purpose (Secondary Purpose) if such Secondary Purpose is compatible with the original Business Purpose. By way of example, UPS may Processor Customer Personal Data for the following Secondary Purposes:

- Transfer Customer Personal Data to an Archive;
- IT systems and infrastructure related Processing such as for maintenance, support, life-cycle management, and security (e.g., resilience and incident management);
- Internal audits or investigations;
- Implementation of business controls and operational efficiency;
- Statistical, historical, or scientific research;
- Dispute resolution;
- Legal or business consulting; or
- Insurance purposes.

Any use of Customer Personal Data for a Secondary Purpose will be assessed on a case-by-case basis by UPS.

4. Processing of Sensitive Personal Data

UPS will not Process Sensitive Personal Data, unless:

- The Processing is necessary for compliance with a legal obligation to which the Controller is subject;

- The Processing is required under a collective agreement;

- The Processing is necessary to protect the vital interests of the Customer or of another person, but only where the person is physically or legally incapable of consenting;

- The Processing relates to Personal Data which have been manifestly made public by the Customer;

- The Processing is necessary for dispute resolution or fraud prevention;

- The Processing is carried out for Secondary Purposes as detailed in Section 3 and where allowed under applicable law.

5. Quantity and Quality of Customer Personal Data

UPS only Processes Customer Personal Data that is necessary and adequate to achieve the applicable Processing Purposes and for only as long as needed for the Processing Purpose. UPS will take steps to delete, anonymize, or destroy Customer Personal Data that is no longer necessary for the Processing Purpose. UPS has fixed data and records retention periods that define for how long Customer Personal Data can be Processed.

UPS will only Process Customer Personal Data that is accurate, complete, and kept-up-to-date. UPS will take steps to rectify or erase Customer Personal Data that is known to be inaccurate without delay.

6. Information and Transparency

UPS informs Customers through its privacy policies and notices of the following information regarding the Processing of their Personal Data:

- Why the Processing is necessary (the Processing Purposes);
- Which categories of Personal Data are Processed;
- The justification of the Processing (the legal grounds for Processing). If the Processing is justified by UPS's legitimate interest, UPS informs the Customers of the legitimate interests pursued by UPS;
- The Group Company that is responsible for the Processing and how it can be contacted;
- To whom the Personal Data is disclosed. If the Personal Data is transferred abroad, UPS informs the Customers of the transfer safeguard used to protect the transfer;
- For how long the Personal Data will be Processed;
- What rights the Customers can exercise with respect to their Personal Data; and
- If automated decision-making (including profiling) is involved in the Processing.

7. Customers Rights

Every Customer has the right to exercise the following rights, in accordance with the procedure outlined in **Annex 2**:

- The right to request confirmation of whether or not their Personal Data is Processed;
- The right to request a copy of their Personal Data;
- The right to request access to the information listed above (Information and Transparency);

- The right to have their Personal Data rectified or completed is such Personal Data is incorrect or incomplete;

- The right to have their Personal Data deleted if such Personal Data is not Processed in compliance with applicable law;

- The right to obtain the restriction of the Processing; and

- The right to object to the Processing (e.g., the right object to receiving marketing communications).

8. Direct Marketing

UPS may send direct marketing communications to Customers only with prior consent. UPS will also always provide Customers with the right to opt-out of future direct marketing communications. UPS will process opt-outs and withdrawals of Customers' consent without undue delay.

9. Automated Decision-Making

Customers have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal (or similar significant) effects on them. This does not apply to such decisions that are necessary to enter or perform a contract with the Customer, if EEA law authorizes it; or if the decision is based on the Customer's explicit consent.

10. Security and Personal Data Breach Notifications

UPS has implemented appropriate measures to protect Customer Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, or access of such Personal Data. UPS only provides its staff access to Customer Personal Data to the extent necessary to achieve the Processing Purpose. Moreover, UPS designs (when determining the means for Processing) and implements (at the moment of the Processing itself), measures to implement the GDPR data protection principes in an effective manner and to integrate the necessary safeguards into the Processing to meet the requirements of the GDPR and protect the rights of Customers.

UPS has designed procedures to document, assess, and report Personal Data Breaches to relevant Supervisory Authorities and, where applicable, affected persons, in accordance with applicable regulatory deadlines.

11. Transfers of Personal Data

UPS will only transfer Customer Personal Data to Controllers or Processors if it is necessary to serve the Processing Purpose and provided transfer safeguards are in place:

- **Transfers to third party Controllers**: Customer Personal Data will only be transferred to a third party Controller if UPS has entered into a valid contract that requires that third party Controller to appropriately protect the privacy interests of the Customer;

- **Transfers to third party or internal UPS Processors**: Customer Personal Data will only be transferred to a third party or internal UPS Processor if UPS has entered into a valid contract with the Processor (Processor Contract). Such Processor Contract must include the following provisions:

    - The Processor only Processes the Customer Personal Data for purposes authorized by UPS and in accordance with UPS's documented instructions (incl. on onward transfers);
    - The Processor keeps the Customer Personal Data confidential and imposes confidentiality obligations on its staff;
    - The Processor implements appropriate technical, physical, and organizational security measures to protect the Customer Personal Data and promptly notifies UPS of any Personal Data Breach involving Customer Personal Data;
    - The Processor only uses Subprocessors that Process Customer Personal Data with the prior written approval of UPS and the Processor imposes data protection obligations on its Subprocessors that are no less protective than those imposed on the Processor under the Processor Contract;
    - The Processor shares with UPS all the information necessary to demonstrate its compliance with its obligations under the Processor Contract and applicable data protection requirements;
    - The Processor handles requests and complaints of individuals as instructed by UPS; and
    - The Processor returns or deletes the Customer Personal Data per UPS's request.

- **Transfers to third parties outside the EEA**: Customer Personal Data will only be transferred to a third party located outside the EEA and not covered by an Adequacy Decision if transfer safeguards providing an adequate level of data protection can be implemented or if the transfer is subject to a derogation for specific situations under EEA data protection law (e.g., if the Customer has explicitly consented to the proposed consent after having been informed of the possible risks of such transfer).

VII. Accountability

UPS has designed a privacy governance program to oversee, manage, and demonstrate compliance with the BCRs. UPS's Business Risk & Compliance Committee (BRCC) is responsible for overseeing the compliance with the BCRs. UPS ensures that adequate measures can be implemented to address any violation of the BCRs identified during the monitoring or auditing of the BCRs' compliance.

UPS's trains its staff that has access to and that processes Customer Personal Data as part of their functions to make sure they can comply with the obligations and principles laid down in the BCRs. Non-compliance by UPS's staff with the BCRs may result in disciplinary action in accordance with UPS policies and local law (up to and including termination of employment or contract).

UPS carries out Data Protection Impact Assessments (DPIA) whenever a Processing is likely to result in a high risk for the rights and freedoms of Customers (e.g., where new technologies are used). Such DPIAs contain descriptions of the envisaged Processing and the Purposes for Processing, an assessment of the necessity and proportionality of the Processing, an assessment of the risks to the rights and freedoms of Customers and the measures envisaged by UPS to address the potential risks.

VIII. Complaints and Enforcement of Rights

Customers can file their complaints in accordance with the procedure outlined in **Annex 2**. Customers can also submit their complaints or claims with:

- The Lead SA or the courts in Belgium, against UPS Europe SRL;

- The SA of the country where the Customer is located or where the infringement took place, against the Group Company that acts as the Controller of the Customer Personal Data or, against UPS Europe SRL; or

- The courts in the country where the Customer is located or where the Group Company that acts as the Controller of the Customer Personal Data is established, against the Group Company that acts as the Controller of the Customer Personal Data or, against UPS Europe SRL.

Customers that file claims are entitled to compensation of damages suffered as a result of the violation of the BCRs, to the extent provided by applicable law of the relevant EEA country. Claim for damages require Customers to demonstrate that they have suffered the relevant damages and to establish facts which show that the damages have occurred because of a violation of the BCRs. It is up to UPS to prove that the damages suffered are not attributable to UPS or a Processor. All Group Companies will cooperate with and assist each other to handle a request, complain, or claim made by a Customer and investigations or inquiries by a competent SA or public authority.

Customers are encouraged to first file their complaints with UPS before reaching out to authorities or courts.

*

* *

Annex 1 – Definitions

- **ADEQUACY DECISION** shall mean a decision issued by the European Commission under EEA Data Protection Law that a country or region or a category of recipients in such country or region is deemed to provide an "adequate" level of data protection.
- **ARCHIVE** shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any Personal Data set that is subject to appropriately enhanced security and has restricted access (e.g., access only by the system administrator).
- **ARTICLE** shall mean an article in the BCRs.
- **BRCC** shall mean the Business Risk & Compliance Committee that oversees respective regional and local compliance and risk programs, including privacy and information security.
- **BUSINESS PARTNER** shall mean any Third Party, other than a Customer or Supplier, that has or has had a business relationship or strategic alliance with UPS (e.g., a joint marketing partner, joint venture, or joint development partner).
- **BUSINESS PURPOSE** shall mean a purpose for Processing Personal Data as specified in Article 2.1 or 2.2 of the full BCRs or for Processing Sensitive Data as specified in Article 2.3. of the full BCRs.
- **COMPETENT SA** shall mean the SA competent to audit under Article 2 of Annex 4 of the full BCRs.
- **CONTROLLER** shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Data.
- **COUNTRY** shall mean each country in which a Group Company is established.
- **CUSTOMER** shall mean any person, private organization, or government body that purchases, may purchase or has purchased a UPS product or service.
- **DATA EXPORTER** shall mean the Group Company that Transfers Personal Data under the BCRs.
- **DATA IMPORTER** shall mean the Group Company that is the recipient of a Transfer of Personal Data under the BCRs.
- **DATA PROTECTION COORDINATOR** shall mean the data protection/GDPR compliance coordinators appointed by the Privacy Coordinators pursuant to Article 3 of Annex 3 of the full BCRs.
- **DATA PROTECTION IMPACT ASSESSMENT** (DPIA) shall mean a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Data, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used. A DPIA shall contain a description of:
    - the scope and context of the Processing;
    - the Business Purposes for which Personal Data are Processed;
    - the specific purposes for which Sensitive Data are Processed;
    - categories of Personal Data recipients, including recipients not covered by an Adequacy Decision;
    - Personal Data storage periods; and
    - an assessment of:
    - the necessity and proportionality of the Processing;
    - the risks to the privacy rights of Individuals; and

    - the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Personal Data.
- **DATA SECURITY BREACH** shall mean the unauthorized acquisition, access, use or disclosure of unencrypted Personal Data that compromises the security or privacy of such information to the extent the compromise poses a high risk of financial, reputational, or other harm to the Individual. A Data Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Data by an Customer of UPS or Third Party Processor or an individual acting under their respective authority, if:
    - the acquisition, access, or use of Personal Data was in good faith and within the course and scope of the employment or professional relationship of such Employee or other individual; and
    - the Personal Data are not further acquired, accessed, used or disclosed by any person.
- **DISCLOSURE REQUEST** shall have the meaning set forth in Article 11.2 of the full BCRs.
- **DIVESTED ENTITY** shall mean the divestment by UPS of a Group Company or business by means of:
    - a sale of shares that results in the divested Group Company no longer qualifying as a Group Company; and/or
    - a demerger, sale of assets, or any other manner or form.
- **EEA** or **EUROPEAN ECONOMIC AREA** shall mean all Member States of the European Union, Norway, Iceland and Liechtenstein and, for the purposes of the BCRs, Switzerland.
- **UPS' General Counsel** can decide to include other countries in this definition, provided that such country is subject to an Adequacy Decision. EEA COUNTRIES shall mean the countries in the EEA.
- **EEA DATA PROTECTION LAW** shall mean provisions of mandatory law of an EEA Country containing rules for the protection of individuals with regard to the Processing of Personal Data including security requirements for and the free movement of such Personal Data.
- **EFFECTIVE DATE** shall mean the date on which the BCRs become effective as set forth in Article 12.1 of the full BCRs.
- **EMPLOYEE** shall mean an employee, job applicant or former employee of UPS. This term does not include people working at UPS as consultants or employees of Third Parties providing services to UPS.
- **GDPR** shall mean 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 (General Data Protection Regulation).
- **GENERAL COUNSEL** shall mean the General Counsel of UPS.
- **GLOBAL PRIVACY OFFICER** shall mean the officer as referred to in Article 1 of Annex 3 of the full BCRs.
- **GROUP COMPANY** shall mean United Parcel Service, Inc. and any company or legal entity of which United Parcel Service, Inc., directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only (i) as long as a liaison and/or relationship exists, and (ii) as long as it is covered by the UPS Policy Book and UPS Code of Business Conduct.

- **IMPORTING GROUP COMPANY** shall mean a Group Company located within a Non-Adequate Country that receives Personal Data from an Exporting Group Company.
- **INDIVIDUAL** shall mean any individual employed by, or any person working for, a Customer, Supplier or Business Partner and any other individual whose Personal Data UPS processes in the context of the provision of its services, including the consignee or recipient of a shipment or delivery.
- **INFORMATION SECURITY AND PRIVACY GOVERNANCE COUNCIL** shall mean the council referred to in Article 2 of Annex 3 of the full BCRs.
- **INTERNAL PROCESSOR** shall mean any Group Company that Processes Personal Data on behalf of another Group Company being the Controller.
- **LEAD SA** shall mean the SA of Belgium.
- **NON-ADEQUATE COUNTRY** shall mean a country that under applicable local law is deemed not to provide an "adequate" level of data protection.
- **ORIGINAL PURPOSE** shall mean the purpose for which Personal Data were originally collected.
- **OVERRIDING INTEREST** shall mean a pressing legitimate need that under specific circumstances outweighs the interest of the Individual.
- **PERSONAL DATA** shall mean any information relating to an identified or identifiable natural person (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), insofar as this information relates to a Customer, Supplier, or Business Partner of UPS or any other individual and is Processed by UPS.
- **PROCESSING** shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.
- **PROCESSING PURPOSES** shall mean the Business Purposes and in respect of Sensitive Data, the specific or general purpose for Processing Sensitive Data listed in Annex 2 (Purposes of Processing) of the full BCRs as well as the Secondary Purposes.
- **PROCESSOR** shall mean Internal Processor or Third Party Processor.
- **PROCESSOR CONTRACT** shall mean any contract for the Processing of Personal Data entered into by UPS and a Third Party Processor.
- **RECORDS OF PROCESSING ACTIVITIES** shall mean a record of Processing activities maintained in writing, including in electronic form, by UPS that contains the following information:
    - the name and contact details of the Group Company that is the Controller;
    - the Processing Purposes;
    - the categories of Personal Data;
    - the categories of recipients to whom Personal Data have been disclosed;
    - where applicable, information about Transfers of Personal Data to a country not subject to an Adequacy Decision;
    - where possible, the envisaged retention periods; and
    - where possible, a general description of the measures under Article 7.1 of the full BCRs.
- **REGION** shall mean a particular geographic area in which certain Countries are grouped.
- **SA** shall mean any supervisory authority of one of the EEA Countries.
- **SECONDARY PURPOSE** shall mean any purpose other than the Original Purpose for which Personal Data are further Processed.

- **SENSITIVE DATA** shall mean Personal Data that reveal an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning an Individual's sex life or sexual orientation, along with Personal Data relating to criminal convictions and offences or social security numbers issued by the government.
- **STAFF** shall mean all current Employees and other persons acting under the direct authority of UPS who Process Personal Data as part of their respective duties or responsibilities towards UPS using Personal Data technology systems or working primarily from UPS's premises.
- **THIRD PARTY** shall mean any person or entity (e.g., an organization or government authority) outside UPS.
- **THIRD PARTY CONTROLLER** shall mean a Third Party that Processes Personal Data and determines the purposes and means of the Processing.
- **THIRD PARTY PROCESSOR** shall mean a Third Party that Processes Personal Data on behalf of UPS and at its direction as a Controller.
- **TRANSFER** shall mean the disclosure of, or remote access to, Personal Data under the BCRs to a Group Company in a country outside the EEA that is not covered by an Adequacy Decision.
- **TRANSFER IMPACT ASSESSMENT** shall mean an assessment on whether, taking into account the specific circumstances of the Transfer, the laws and practices of the third country of destination to which Personal Data are Transferred (Third Country), including those requiring the disclosure of Personal Data to public authorities or authorizing access by such authorities, prevent UPS from fulfilling its obligations under the BCRs. In assessing the laws and practices of the Third Country, UPS shall take into account in particular:
    - the specific circumstances of the Transfers, and any envisaged onward Transfers within the same Third Country or to another Third Country, including:
      i. purposes for which the data are Transferred and Processed;
      ii. types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfers);
      iii. sector in which the Transfers occur;
      iv. categories and format of the Personal Data Transferred;
      v. location of the Processing including storage; and
      vi. transmission channels used.
    - the laws and practices of the Third Country relevant in light of the circumstances of the Transfers, including requirements to disclose Personal Data to public authorities or authorizing access by such authorities as well as the applicable limitations and safeguards. This also includes laws and practices providing for access to Personal Data during transit between the country of the Data Exporter and the Third Country; and
    - any relevant contractual, technical or organizational safeguards put into place to supplement the safeguards under this Code, including measures applied during transmission and to the Processing of Personal Data in the Third Country.
- **UPS** shall mean United Parcel Service, Inc. and its Group Companies.
- **UPS EUROPE SRL** shall mean UPS Europe SRL, having its registered seat in Brussels, Belgium.
- **INTERPRETATION OF THESE BCRs**:
    - Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in the full BCRs, as they may be amended from time to time;

- headings are included for convenience only and are not to be used in construing any provision of the BCRs;
- if a word or phrase is defined, its other grammatical forms have a corresponding meaning;
- the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;
- a reference to a document (including, without limitation, a reference to the BCRs) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by the BCRs or that other document;
- a reference to law or a legal obligation includes any regulatory requirement, sectorial guidance, and best practice issued by relevant national and international supervisory authorities or other bodies; and
- Terms that are not defined in the BCRs have the meanings given to them in the GDPR.

Annex 2 – Procedure for Customers' Requests and Complaints

1. Procedure

Customers should send their request to the contact person or contact point indicated in the relevant privacy policy or notice. Customers also may send their request to the office of the Global Privacy Officer via email to globalprivacy@ups.com.

Prior to fulfilling the request of the Customer, UPS may request the Customer to:

- specify the categories of Personal Data to which he or she is seeking access;
- specify, to the extent reasonably possible, the system in which the Personal Data are likely to be stored;
- specify the circumstances in which UPS obtained the Personal Data;
- provide proof of his or her identity when UPS has reasonable doubts concerning such identity, or to provide additional information enabling his or her identification;
- pay a fee to compensate UPS for the reasonable costs relating to fulfilling the request provided UPS can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character; and
- in case of a request for rectification, deletion, or restriction, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with EEA Data Protection Law or the BCRs.

2. Response Period

Within one calendar month of UPS receiving the request and any information necessary under Section 1 above, UPS shall inform the Customer in writing or electronically either (i) of UPS's position with regard to the request and any action UPS has taken or will take in response, (ii) a specification of the information necessary for UPS to comply with the request in accordance with Section 1 above or (iii) the ultimate date on which he or she will be informed of UPS's position and the reasons for the delay. UPS may extend the original one-month response period by two calendar months where necessary, taking into account the complexity and number of the requests.

3. Complaints

A Customer may file a complaint in accordance with Article 10.1 of the BCRs and/or file a complaint or claim with the authorities or the courts directly, in accordance with Article 10.2 of the BCRs if:

- the response to the request is unsatisfactory to the Customer (e.g., because the request is denied);
- the Customer has not received a response as required by Article 2;
- the time period provided to the Individual in accordance with Article 2 is, in light of the relevant circumstances, unreasonably long, and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response; or
- UPS violates the Customer's rights under the BCRs.

4. Denial of Requests

Customer' requests are subject to any applicable exceptions provided under EEA Data Protection Law. Applying exceptions requires the prior consultation of the relevant Privacy Coordinator. Depending on the relevant right of the Customer, UPS may deny the request of the Customer in accordance with EEA Data Protection Law only, for example where:

- the request does not meet the requirements of the corresponding rights as set out in Articles 5.1 - 5.3 of the BCRs;
- one of the exemptions of Article 5.4 of the BCRs apply;
- in case UPS processes a large quantity of information concerning the Employee, the request is not sufficiently specific;
- the identity of the relevant Customer cannot be established by reasonable means, including additional information provided by the Customer;
- UPS can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character. A time interval between requests of six months or less shall generally be deemed to be an unreasonable time interval;
- the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of UPS;
- the Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;
- the Processing is necessary for exercising the right of freedom of expression and information;
- for dispute resolution purposes;
- in so far as the request violates the rights and freedoms of UPS or others; or
- in case a specific restriction of the rights of Customer applies under EEA Data Protection Law.