AGREEMENT REGARDING COMMISSIONED DATA PROCESSING (JANUARY 2019)

General

The provisions of this Agreement regarding Commissioned Data Processing shall apply as between DHL Paket GmbH (hereinafter referred to as the 'Processor ') and its customer (hereinafter referred to as 'Controller(s)') for managing personal data in the online systems provided for dispatch preparation in addition to the data processing required for providing postal services. This Agreement shall apply solely to the extent that Controllers use the address book functions provided by DHL Paket GmbH to permanently manage their customer addresses independent of mail-shots.

Subject matter of the processing

With its online systems, specifically the DHL Business Customer Portal, DHL Pickup System, DHL Returns Portal and DHL Supplier Portal, DHL Paket GmbH provides Controllers with additional functions, which are not required for providing postal services, for permanently managing their customer address independent of mail-shots (hereinafter referred to as 'Address Book Functions').

Term

This Agreement regarding Commissioned Data Processing shall apply for an indefinite period and may be terminated at any time by discontinuing use of the Address Book Functions and deleting all stored data in the Address Book Functions.

Specifications for the processing

1. Nature and purpose of the intended processing
   Use of the Address Book Functions is optional and serves the purpose of permanently managing the Controller's customer addresses independent of mail-shots. The Controller itself inputs, modifies, stores and deletes the data. Use of these Address Book Functions is not required for providing postal services, rather it merely assists the Controller with managing its dispatch addresses.

2. The data processing activity agreed upon shall be carried out solely within the EU/EEA . Any transfer of personal data outside the EU/EEA shall require the prior (written (including by e-mail)) consent of the Controller and then only provided that the requirements set out in Article 44 et seq. of the EU General Data Protection Regulation (GDPR) have been met.

3. Types of data
   The following types/categories of personal data will be processed:
   - Name
   - Contact data
   - Adress

Technical and organizational measures

(1) Taking into account the state of the art, the costs of implementation and the nature, scope and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures in a manner so as to ensure that processing personal data meets the requirements of applicable data protection laws, specifically those of the GDPR and this Agreement. The Processor hereby acknowledges and ensures the aforementioned rights of the data subjects. To this end and in accordance with Article 32 GDPR, the Processor shall take technical and organizational measures and hereby confirms the implementation thereof.

(2) The measures to be taken are data security measures and measures to ensure a level of security appropriate to the risk with respect to confidentiality, integrity, availability and resilience of the systems. The state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of likelihood and severity for the rights and freedoms of natural persons within the meaning of Article 32 (1) GDPR shall be taken into account.

(3) The technical and organizational measures change as the state of the art progresses and will be enhanced consistently. The Processor may take appropriate alternative measures in this regard, provided that the level of security of the stipulated measures agreed upon herein is maintained.

(4) Notwithstanding the foregoing, the Processor shall introduce a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing agreed upon herein.

Rectification, restriction and erasure of data

(1) The Processor may rectify, erase or block personal data only on instructions from the Controller. If a data subject submits a request for rectification or erasure of personal data directly to the Processor, the Processor shall forward such request to the Controller without undue delay.

(2) The Processor shall assist the Controller, insofar as this is possible, with fulfilling the Controller's obligation to respond to requests for exercising the data subject's rights. These rights include the 'right to be forgotten' as well as the right to rectification, data portability and the right of access.

(3) The Processor shall not be liable for the Controller's failure to respond to the request of a data subject correctly, in due time, or at all.

Obligations of the Processor

In addition to the provisions and obligations set out in this Agreement, the Processor shall comply with the statutory provisions under Articles 28-33 GDPR. In light of the foregoing, the Processor shall in particular

(1) process the personal data only on documented instructions from the Controller, unless required to do so by applicable laws to which the Processor is subject; in such a case, the Processor shall to the extent

permitted by law inform the Controller of that legal requirement before processing the personal data. The Processor shall confirm oral instructions in writing or by e-mail without undue delay;

(2) inform the Controller without undue delay if, in its opinion, an instruction infringes the provisions of data protection law. In such case, the Processor may suspend execution of the relevant instruction until it has been confirmed or modified by the Controller;

(3) appoint a data protection officer or, if the Processor is not required to appoint a data protection officer, specify another contact person responsible for data protection matters;

(4) maintain a record of processing activities;

(5) grant access to the personal data only if and to the extent that such access is prescribed and necessary for providing the services and where the relevant employees and advisers have signed appropriate confidentiality agreements and have committed themselves to confidentiality.

The Processor and any person acting under the authority of the Processor and/or of the Controller, who has access to personal data, shall not process those data except on instructions from the Controller, unless required to do so by law;

(6) inform the Controller without undue delay of any inspections, investigations and/or administrative measures by a supervisory authority to the extent that these relate to the subject matter of this Agreement and this is permitted by law;

(7) where the Controller is subject to an investigation by the supervisory authority, administrative or criminal proceedings, liability claims of data subjects or any third party or any other claims in connection with this Agreement and the processing by the Processor, give its best efforts to support the Controller in this regard;

(8) inform the Controller as soon as possible of any complaints, applications or requests or other communications from data subjects, data protection authorities or third parties in connection with processing personal data by the Processor and/or the Controller. Insofar as the Controller is obliged under applicable data protection law to respond to a request from a data subject in connection with processing that data subject's data, the Processor shall support the Controller in transferring the requested information. However, the Processor shall not be required to respond directly to requests of data subjects; it need only refer the data subject to the Controller.

Subcontracting

(1) The Processor may not engage any additional processor (i.e., subcontractor) without the prior express written consent of the Controller.

(2) Where the Processor engages an additional processor for carrying out specific processing activities on behalf of the Controller, the same obligations as set out in this Agreement shall be imposed on that additional processor.

(3) The Controller hereby consents to the addition of subcontractors on the basis of the provisions contained in this clause. The Processor shall inform the Controller in good time before adding or replacing subcontractors, by giving reasonable advance notice of a new additional processor (including full de-

tails of the processing carried out by the new processor). The advance notice shall be effected via the DHL Business Customer Portal.

(4) Before any additional processor processes personal data of the Controller for the first time, the Processor shall carry out an appropriate due diligence to ensure that the additional processor is in a position to offer the level of protection for the Controller's personal data prescribed by this Agreement, the services agreement and applicable law.

(5) If the Controller has legitimate objections to Processor's use of an additional processor, the Controller shall notify the Processor thereof immediately in writing within five business days of receipt of the Processor's notification. For the avoidance of doubt, the parties agree that objections by the Controller shall not be legitimate if the additional processor has passed the security audit for the Processor's suppliers - unless the Controller can demonstrate that the new processor constitutes an unreasonable risk to the protection of personal data (e.g., if the additional processor has violated security regulations in the past) or is a competitor of the Controller.

(6) Notwithstanding the foregoing, if the Controller objects to the engagement of an additional processor, the parties shall consult in good faith to arrive at an appropriate solution. The Processor may in particular decide (i) not to use the intended processor or (ii) to take the corrective action requested by the Controller and engage the processor. If none of the aforementioned options or some other option is reasonably feasible and the Controller still has legitimate objections, the Controller may rescind this Agreement by deleting all stored data and discontinuing use of the Address Book Functions.

(7) If and to the extent that outsourced ancillary services are involved, the Processor shall make appropriate and lawful contractual agreements and take appropriate control measures to ensure adequate protection and security of the Controller's data.

Audit rights

(1) Subject to reasonable advance notice from the Controller of at least ten business days and to ensure and review compliance with the technical and organizational security measures and the obligations arising under this Agreement, the Processor shall permit the Controller or another auditor mandated by the Controller to carry out audits if

   a. the Controller has reason to suspect that the Processor is not acting in compliance with the technical and organizational measures and/or the obligations hereunder;

   b. a security event occurs;

   c. the Controller's supervisory authority responsible requires such audit.

(2) Notwithstanding the foregoing, compliance with the provisions may be demonstrated by

   a. adherence to approved codes of conduct; and/or

   b. certification in accordance with an approved certification mechanism pursuant to Article 42 of the GDPR; and/or

   c. current attestations, reports or excerpts of reports by independent bodies. Upon the Controller's request, the Processor shall provide the Controller with a copy of the audit report signed by the external auditor so that the Controller can adequately verify that the Processor is implementing or performing the technical and organizational measures and obligations under this Agreement.

(3) Audits will be carried out during normal business hours, with an appropriate scope and without disrupting business operations. In the event that the Controller engages an independent auditor to perform the audit, such independent auditor shall sign a nondisclosure agreement first. The independent auditor may not be a competitor of the Processor.

(4) If the audit causes the Processor or any additional processor to incur expenses in excess of one business day, the Controller agrees to reimburse the expenses for each day in excess thereof.

Obligation to provide support

(1) The Processor shall support the Controller in complying with the obligations set out in Articles 33 to 36 GDPR concerning the security of personal data, notification obligations in the event of personal data breaches, data protection impact assessments and prior consultations. This shall include, in particular

a. reporting personal data breaches to the Controller without undue delay;

b. supporting the Controller in its duty to inform the data subject and providing the Controller with all relevant information without undue delay in this connection;

c. supporting the Controller with data protection impact assessments;

d. supporting the Controller with the record of processing activities;

e. supporting the Controller with consultations with the supervisory authority.

(2) The Processor may claim remuneration for the support services set out in paragraph 1 (c) and (d).

Erasure and return of personal data

(1) After completing the contractually agreed upon work, or prior thereto at the Controller's request, albeit not later than upon the termination of the use of the Address Book Functions, the Processor shall confirm erasure of the personal data to the Controller.

(2) Records serving to document proper data processing shall be retained by the Processor in accordance with the respective retention periods. The Processor may discharge its obligations by turning them over to the Controller upon completion of the services.

Dispute resolution

Exclusive place of jurisdiction for disputes arising out of this Agreement and any individual contracts of carriage within the scope of this Agreement shall be Bonn (Germany). The Agreement shall be governed by German law.

Miscellaneous

(1) Should the Controller's data be the subject of an investigation and seizure, an order of attachment, confiscation in connection with bankruptcy or insolvency proceedings or similar events or third party actions whilst those data are within the Processor's sphere of control, the Processor shall notify the Controller thereof without undue delay. The Processor shall notify all parties to such action without undue delay that the data concerned are the exclusive property of and within the sphere of control of

the Controller, that the Controller has the sole right to dispose over such data and that the Controller is responsible for the application of data protection law.

(2) Should any provision of this Agreement be deemed invalid, unlawful or unenforceable for whatever reason, the relevant provision shall be excluded and the remaining provisions of this Agreement shall be given full force and effect as if this Agreement had been executed without the invalid provision.

(3) This Agreement is governed by the laws of the Federal Republic of Germany.

Annex 1: technical and organizational

Within its sphere of responsibility, DHL Paket GmbH takes the following technical and organizational measures when processing personal data.

Physical access control

Objective:
Prevent unauthorized people from gaining access to the data processing equipment by means of which personal data is processed or used.

Principles:

- Establishment of various security zones (SK1 - SK4). A distinction is generally made between public areas, office space and technical space (data centres, network rooms).
- Appropriate measures are in place for controlling physical access between security zones with different security classifications.
- A formal procedure for assigning/changing/revoking access authorization is in place.
- A formal procedure for escorting visitors and external personnel is in place.

Measures:

- Monitored personal interlocks to the security areas
- Security areas have been defined
- People authorized to access those areas are identified by means of machine-readable IDs.
- Locking policy according to company rules
- Wearing of company badges is monitored constantly by security personnel.
- Outer perimeter secured by special structural measures, alarm systems, burglar alarm system, watch guards.
- Entries and exits are logged.

2. System access control

Objective:
Prevent data processing systems from being used by unauthorized people.

Principles:

- Users must always identify themselves individually.
- Authentication, i.e., verification of the presented identification, is password-based, at a minimum.
- The quality (structure, length etc.) of passwords and the basic conditions for their use (storage, transfer etc.) comply with the applicable security standards.
- System and data access authorization are checked periodically, at least once a year, to ensure they are up to date and valid. Audit-compliant event logs are kept.
- Operating processes have been established to create, revoke or change access authorization.

Measures:

- Transmission lines secured by special structural measures.

- User and access control measures are in place for all parts of the enterprise.
- The network is secured by means of firewall systems with regard to the internet and other networks.
- Password procedure is in place for secure identification with subsequent user authentication.
- Policy-enforced locking of workstations upon leaving the workplace (e.g., password or screen lock)
- User administration with authorization levels
- Policy-enforced process for assigning, checking and revoking access authorization.
- Administrative access to systems is secured at the network level.

3. Data access control

Objective:
Ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after storage.

Principles:

- The standard user has no write access to system files and no administrator privileges.
- Where technically feasible, central user administration is installed.
- Administrator accounts such as root and DBA are personalised. If this is not possible with the objects used, suitable processes or tools such as sudo with Unix are used.
- Administrator access to systems in customer environments is secured at the network level by appropriate security mechanisms.

Measures:

- Defined, audit-compliant authorisation concepts for system, database and application level
- Authorisation concepts include, inter alia, the process description of the assignment and revocation of rights based upon the dual control principle and the ‘need to know’ principle for access to resources and information
- Differentiated access authorisation (profiles, roles)
- Policy-enforced process for assigning, checking and revoking access authorisation
- Identification and authentication of users in accordance with the authorisation concepts and process flows for changing authorisation concepts. Identification and authentication of system and database administrators
- Password policy with defined validity periods and documentation of password history
- Logging of authorised users and their login/logouts
- Encryption of files where necessary

Disclosure control

Objective:

Ensure that personal data cannot be read, copied, altered or removed without authorization when being transferred electronically, transported or stored on data storage media and that it is possible to check and ascertain at which point personal data are to be transmitted by data communication equipment.

Principles:

- Safety-relevant system-related events and accesses to the system are logged (system log) and transaction logs are retained for ninety days. No user activities beyond this are logged.
- Transaction logs are analysed on a case-by-case basis, taking into account legal requirements.
- Transaction logs are backed-up using the regular backup procedure. Transaction logs are only restored using the established change procedure.
- The encryption technologies used are based upon proven and recognised standard procedures and proposed minimum key lengths.
- The application must be able to take into account a change in the key length.
- Confidential data may only be stored on mobile data storage media in encrypted form.

Measures:

- Data storage media are sent in sealed transport containers.
- Secure or encrypted transmission channels
- Logging by active network components and, if necessary, analysis by the network centre
- Controlled destruction of data storage media
- State-of-the-art encryption technology

Input control

Objective:

Ensure that it is possible after the fact to check and ascertain whether and by whom personal data have been entered, changed or removed in data processing systems.

Principles:

- For the secure operation of an application, a security concept is available that includes at least the following points:
  - An authorization concept has been created and a corresponding user administration has been set up.
  - User accounts in the application do not use hard-coded passwords or hard-coded user IDs.
  - Passwords are stored and transferred in cryptographically encrypted form.
- Security features of the respective programming languages and tools must be used and may not jeopardise or influence the security of the underlying system.
- All development and test-specific logging processes are deactivated or removed before the software is released into the operating process.
- Safety-relevant system-related events and accesses to the system are logged (system log) and transaction logs are retained for ninety days. No user activities beyond this are logged.
- Transaction logs are analysed on a case-by-case basis, taking into account contractual and legal requirements.
- Transaction logs are backed-up using the regular backup procedure. Transaction logs are only restored using the established change procedure.

Measures:

- Proof of organisationally defined input responsibilities

- Identification and authentication of users in accordance with the authorisation concepts
- Authentication concept
- Logging and log analysis
- Secure log files against unauthorised use and modification

Job control

Objective:
Ensure that personal data processed on behalf of a customer may only be processed in accordance with the customer's instructions.

Principles:

- Pursuant to Article 28 of the GDPR, the Processor collects, processes and uses personal data solely on instructions of the customer. Apart from instructions, the Processor does not use the data provided for collection, processing or use for its own purposes or for the purposes of third parties (principle of purpose limitation). If the Processor is of the opinion that an instruction breaches data protection provisions, the Processor must advise the customer thereof in writing.
- The Processor only uses staff who have signed appropriate confidentiality agreements and have committed to postal secrecy pursuant to section 39 of the Postgesetz (PostG - German postal act) and to telecommunications secrecy pursuant to section 88 of the Telekommunikationsgesetz (TKG - German telecommunications act) (within the scope of the TKG). The original undertakings will be submitted as templates on request for audit purposes during audits.
- The Processor informs the customer in writing of any disruptions to processing, suspected data breaches and other irregularities in the processing of the customer's personal data.
- The customer has the right to verify compliance with the applicable data protection regulations and data security measures with regard to the processing of its data after prior consultation with the Processor's data protection officer.
- The Processor engages suppliers to collect, process or use personal data exclusively within the scope of an agreement for commissioned data processing in accordance with Article 28 of the GDPR.
- Job control takes place on the basis of an established framework at the Processor for implementing the statutory and group requirements in the context of commissioned data processing.

Measures:

- Application ensures that personal data are collected, processed and used exclusively within the Controller's sphere of control
- Formalised commissioning process
- Measures to monitor proper performance of the agreement

Availability control

Objective:

Ensure against accidental loss or destruction of personal data.

Principles:

- Data storage media are stored exclusively in the robotic system or in the security archive.
- All incoming and outgoing data storage media are stored in the security archive.

Measures:

- A data backup concept has been established.

Purpose limitation control

Objective:

Ensure that data collected for different purposes can also be processed separately for the respective purpose.

Principles:

- Every newly developed system or application must undergo the Privacy & Security Assessment (PSA) procedure. All changes must be considered in the PSA review.
- Approval procedures for transfer to production are used.
- Development is carried out on standard systems with current patch versions and standard security settings, if technically feasible and approved by the customer.
- Dependencies to the operating system and the middleware used are co-ordinated and documented.
- Application-specific security-relevant settings are documented accordingly in the application's security concept.
- Development, testing and acceptance systems are operated in independent network segments insofar as this is technically feasible and contractually stipulated.
- Testing and production data are segregated.
- Personal data will be anonymised or pseudonymized prior to use as test data, insofar as this is possible according to the intended purpose and does not require disproportionate effort in relation to the envisaged protective purpose.

Measures:

- Logical segregation of the database
- Physical segregation of the storage media
- Anonymization or pseudonymization of test data
- Segregation of testing, development and production environments
- Guidelines and work instructions for development and operation

DEFINITIONS AND CONSTRUCTION

Term	Definition
Agreement	Agreement means this Agreement including its Annexes.
Ancillary services	Ancillary services means services which are provided independently of the subject matter of this Agreement, such as telecommunications services, postal/transport services, maintenance and support services for users or the disposal of data storage media as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.
Annex	Annex means any Annex to this Agreement which shall constitute an integral part thereof.
Additional processor	Additional processor means any data processor engaged by the Processor in the course of providing the services.
Controller	Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data protection laws	Data protection laws means the European Union data protection laws and the data protection laws of another jurisdiction, where applicable.
EEA	EEA means the European Economic Area and comprises all the member states of the European Union, Liechtenstein, Norway and Iceland.
GDPR	GDPR means Regulation (EU) Number 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).
Personal data	Personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
Services	Services means any and all services provided by the Processor as agreed in the services agreement.
Services agreement	Services agreement means the agreement entered into by the parties for the provision of services by the Processor.