DHL GROUP
DATA PRIVACY POLICY

Global Data Protection
Version: 2.2 July 2023

PUBLIC

Table of Content

PREAMBLE

1. The use of modern information and communication technologies and the global networking of information flows are fundamental to the business processes of DHL Group. Particularly, complex organisational structures and the challenge to be able to run the necessary applications on a 24 hour basis require an international IT infrastructure in which personal data is processed on a group wide level. With this in mind, the protection of the personal data of customers, employees, shareholders and business partners is an essential global concern of all companies within DHL Group.

2. The aim of this DHL Group Data Privacy Policy is to establish a standardized, adequate, and global data protection and data security standard for DHL Group as a whole. In particular, the aim is to guarantee adherence to legal requirements for cross-border data traffic, as well as to ensure adequate protection for data subjects in the internal, cross-company processing of personal data. DHL Group Data Privacy Policy thus contributes, and forms part of the data protection accountability measures taken by the DHL Group.

3. The companies of DHL Group are aware that, in their customers' view, they are perceived as a single unit in many areas and therefore pledge to share responsibility for implementing the DHL Group Data Privacy Policy by handling personal data in a reliable and secure manner in order to contribute to the commercial success of the Group.

I. SCOPE

1. Area of application

(1) The DHL Group Data Privacy Policy applies to the processing of personal data of natural persons, in particular the data of customers, employees, shareholders and business partners aiming at creating an adequate level of protection for the transfer of personal data from Group companies established in the European Union to Group companies in a third country without an adequate level of protection. The natures of the processed data, as well as the purposes of processing, depend on the relationship individual data subjects may have with one or more DHL Group companies. The information in question is mainly connected, e.g. to the handling of employment relationships covering a wide range of possible aspects from starting of work to possible career and development opportunities, as well as customer relationship management which may include a variation of customer services [1].

(2) The DHL Group Data Privacy Policy does not apply to data transfers which are covered by derogations stipulated in Article 49 sec. 1 of the General Data Protection Regulation (GDPR), e.g. when a data subject has given his consent or when the transfer is necessary for the performance of a contract. Also, the DHL Group Data Privacy Policy does not apply to statistical analyses or studies performed on the basis of anonymized or pseudonymized data that do not allow conclusions to be made about data subjects.

2. Legally binding effect

(1) The DHL Group Data Privacy Policy within DHL Group entered into force upon authorization by the Group's Board of Management and upon publication.

(2) The DHL Group Data Privacy Policy becomes binding for the individual Group companies as soon as the management of the companies in question commits to comply with the regulations in a Declaration of Accession.

(3) The binding effect will end upon revocation of the DHL Group Data Privacy Policy or if the respective company withdraws from the Group. In respect of the data transferred up to this time, the Group companies in question are subject to the obligation to observe the provisions, contained in the DHL Group Data Privacy Policy, on handling personal data. Any further/future data transfers from and/or to Group

[1] DHL Group is built upon two strong pillars: an integrated international logistics business and a solid mail business. DHL Group, consisting of 870 Group companies and a workforce of some 500,000 in more than 220 countries and territories, provides transport services for letters, parcels, goods and information. Business activities which may have an impact on the nature and the purpose of data transfers are described in detail in the annual report. The parent company of the Group is Deutsche Post AG which, together with the headquarters, is located in Bonn (Germany).

companies may only take place if other adequate safeguards as stipulated by Article 46 GDPR are adduced.

3. Relationship to legal regulations

(1) The principles of the DHL Group Data Privacy Policy do not replace the necessary legitimization, under law if applicable, for the processing of personal data, but ensure compliance with specific requirements under the GDPR in the context of cross-border data transfers to third countries. Therefore, any (stricter) national regulations prevail over the requirements stipulated in this Data Privacy Policy.

(2) Within the area of application of the GDPR, the permissibility of the processing of personal data may still be governed by the respective national law where allowed by the GDPR. This shall also apply to the cross-border transfer of data within this area. When data is processed across borders on behalf of the controller in this area, the laws that apply in the controller's location shall be authoritative for the processor.

(3) The admissibility of data processing in relation to data transfers to third countries and to all cross-border data transfers shall be governed by the laws of the country in which the data exporter has its registered office.

(4) The admissibility of processing and transfer of personal data which have not been processed within the scope of the GDPR remains governed by the national laws of the relevant country of processing.

(5) Each Group company is responsible for checking the admissibility of data processing, including any existing requirements to notify national supervisory authorities or inspection offices, according to relevant national and local laws. In cases of doubt, the relevant Data Protection Official or Data Protection Advisor may be consulted for advice.

(6) Obligations and regulations applicable to individual Group companies which relate to the processing and use of personal data, go beyond the following principles and contain further requirements for processing and use of personal data shall remain unaffected by the DHL Group Data Privacy Policy. Nevertheless, companies agree that the laws applicable to the individual companies will not prevent them from fulfilling their obligations as stipulated in the DHL Group Data Privacy Policy.

(7) The collection of personal data and/or its transfer to state offices shall only take place according to the relevant national regulations.

(8) The DHL Group Data Privacy Policy is subject to German law in all other respects.

II. PRINCIPLES

1. Transparency of data processing

(1) Data subjects must be suitably informed of how their personal data is handled. This also includes the publication of the DHL Group Data Privacy Policy in Smart Connect as well as a summary of the policy on the external corporate website.

(2) The duty to inform contains the following details:

- The identity of the legal entity (Group Company) responsible for processing personal data, and its contact details (controller).

- The contact details of the data protection officer, where applicable.

- The purpose and scope of data processing.

- The legal basis for the data processing.

- The legitimate interests where processing is based on these.

- The recipients or categories of recipients of the personal data.

- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.

- The existence of a right to object where data processing is based on legitimate interests.

- Where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- The right to lodge a complaint with a supervisory authority.

- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- Where personal data have not been obtained from the data subject, the categories of personal data concerned and from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

- Where it is intended to further process the personal data for a purpose other than that for which the personal data were collected, the data subject shall be provided prior to that further processing with information on that other purpose.

- Rights of the data subject (see section 5).

(3) The information may be omitted if:

- the data subject already has the information.

- where personal data have not been obtained from the data subject, the provision of such information proves impossible or it would entail a disproportionate expense,

- obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests, or

- the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

(4) The information must be available to the data subject the first-time data is collected. Where personal data have not been obtained from the data subject information shall be provided at the latest within one month after obtaining the personal data, having regard to the specific circumstances. If the personal data are to be used for communication with the data subject, controller shall provide information at the latest at the time of the first communication to that data subject and if a disclosure to another recipient is envisaged, controller shall provide information at the latest when the personal data are first disclosed.

2. General admissibility requirements for the processing of personal data

2.1 Principle

Personal data must be processed lawfully and fairly based on legal allowance or consent. The data must be factually correct and – if applicable – up-to-date. Suitable measures must be taken to ensure that irrelevant or incomplete data is rectified or deleted. The data must be deleted as soon as it is no longer required for the purpose – for which it was originally collected and stored – observing the legal storage obligations.

2.2 Data minimization / data avoidance

Data processing must follow the objective of only processing personal data which is required. Taking account of the intended purpose for using personal data, the data must be appropriate and relevant and must not go beyond the required scope (data minimization). Personal data may only be processed within a specific application if this is necessary (data avoidance).

2.3 Anonymization / Pseudonymization

Where possible and financially feasible, anonymization or pseudonymization methods must be used. Both methods must be undertaken in such a way that the actual identity of the data subject cannot be re-identified or can only be re-identified again with a disproportionate amount of effort.

2.4 Purpose limitation

Personal data may only be collected and processed for specified, explicit and legitimate purposes. It may only be used for the purpose for which it was originally collected. Changes to the purpose are only admissible with the consent of the data subject if permitted by the national law of the data exporter or where processing for another purpose is compatible with the purpose for which the personal data are initially collected.

2.5 Consent

(1) The consent of the data subject must be obtained no later than the date on which the processing of personal data begins.

(2) The consent must be freely given, specific and on an informed basis as an unambiguous indication, which clearly shows the extent of the consent and the possible consequences of withholding consent to the data subject. The formulation of the declaration of consent must be sufficiently clear and inform the data subject of his/her right to revoke his/her consent at any time in the future.

(3) The consent must be obtained in a manner befitting the circumstances (in writing or electronically, verifiably). In exceptions, it may be given verbally if the fact of the consent and the particular circumstances which allow verbal consent are documented sufficiently. If the consent is given in writing together with other declarations, it must be clearly highlighted.

2.6 Tie-in ban

The use of services or the receipt of products and/or services must not be made dependent on the data subject giving his/her consent to the use of his/her data for purposes other than the establishment and performance of the contract. This only applies if the use of comparable services or the acquisition or use of comparable products is not reasonably possible or possible at all for the data subject.

2.7 Data processing on behalf of controller

(1) If a Group company processes personal data on behalf of another Group company, the obligations of the contractor, as a processor of commissioned data, must be referred to in the contract between the controller and processor meeting the requirements of Article 28 GDPR, in addition to the services to be provided in writing or in another equivalent form (Controller-Processor Agreement). In particular the controller must oblige the processor to process personal data solely on its instructions and to take the necessary technical and organizational measures to protect the data.

(2) Without the prior authorization of the controller, the processor may not use the personal data, which was passed on to it, for its own or a third party's purposes. The above regulations must be agreed at least to the same extent with any sub-processor commissioned by the processor. The processor and any sub-processor must be selected according to their ability to meet the above requirements.

(3) If agreements are concluded with processors and/or sub-processors in countries without an adequate data protection standard and not falling under the scope of this DPDHL Data Privacy Policy, adequate safeguards as stipulated by Article 46 GDPR must be obtained with respect to the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

2.8 Onward transfer to third parties

(1) When the data importer transfers personal data to other third parties that have their registered office in the third country or engages in the cross-border transfer of personal data, the data importer shall ensure that this data is processed lawfully. Accordingly, before the onward transfer, suitable data protection and data security measures must be agreed with the recipient which provide for adequate safeguards as stipulated by Article 46 GDPR. These measures will also apply in the case of any further onward transfer.

(2) If personal data which has been processed under the scope of the GDPR is transferred onward to legal entities which are not subject to the DHL Group Data Privacy Policy or to third parties in third countries (onward transfer to non-signatories) without an adequate level of protection, adequate safeguards as stipulated by Article 46 GDPR must be adduced. Notwithstanding the foregoing, personal data may only be transferred within the framework of the GDPR or within the framework of the national regulations passed on the basis of the GDPR.

(3) The above provision will not apply if there are national regulations, particularly for reasons of national security, defense, public safety or the prevention, ascertainment and prosecution of criminal acts, which expressly provide for the transfer of personal data for these reasons.

2.9 Accountability

(1) Each DPDHL Group entity shall ensure and be able to demonstrate compliance with applicable requirements under this Policy.

(2) In particular and where applicable, the controller shall implement appropriate technical and organizational measures, which are designed to implement data protection principles, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects (Principle of data protection by design).

(3) Where applicable, the controller shall 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 (Principle of data protection by default).

3. Special data processing cases

3.1 Special categories of personal data

(1) The processing of special categories of personal data is forbidden unless the processing of such data is necessary, and the data subject explicitly consents to it. In addition, special personal data may only be processed within the framework of the exceptions specified in the GDPR or within the framework of the national exception regulations passed on the basis of the GDPR.

(2) Before such processing begins, the Data Protection Official (Data Protection Officer/Data Protection Coordinator) of the company in question must be involved in accordance with the company's internal regulations.

3.2 Automated decisions in individual cases

(1) Decisions which assess the individual aspects of a person, and which may entail legal consequences for, or considerably affect the data subject, may not be based solely on automated processing unless this is necessary for entering into, or performance of, a contract between the data subject and a data controller, is authorized by Union or Member State or is based on the data subject's explicit consent.

(2) If, in individual cases, it is thereafter justified to make automated decisions, the data subject must be informed about the result of the automated decision and must be allowed to comment on it within a suitable period. His/her comments must be taken into account in an appropriate manner before a final decision is made.

(3) In the case of automated decisions based on special categories of personal data these are only permissible if based on consent of the data subject or on the basis of Union or Member State law.

3.3 Direct marketing

It is generally permitted to process personal data for direct marketing/market or opinion research reasons unless the national law or particular agreements on secrecy/confidentiality stipulate stricter regulations (e.g. need for consent). The data subject has the right to object to the processing of his/her data for this purpose and must be informed separately of this as per section 1. If the data subject objects, the data must be restricted and must not be processed for this purpose.

4. Data quality/data security

4.1 Confidentiality of data processing

Only authorized employees especially committed to the observance of data protection may process personal data. It is forbidden for an employee to process this personal data for his/her own (private) purposes, to transfer it to unauthorized parties or to make it accessible to them in any other way. In this context, “unauthorized” may include colleagues or employees if they do not need the data for their field of work or specialist tasks.

4.2 Principles of data security (technical and organizational measures)

(1) If personal data is processed, taking into account the risks presented by the processing suitable technical and organizational measures must be taken to protect the company processes and IT systems, in order to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

(2) These measures include:

- Refusing unauthorized persons entry to data processing facilities where personal data is processed or used (entry control),

- Preventing unauthorized persons from being able to use data processing systems (usage control),

- Guaranteeing that authorized users of a data processing system can only access data within the scope of their access rights, and that personal data cannot be read, copied, changed or removed without authorization, either during processing or use or when stored (access control),

- Guaranteeing that personal data cannot be read, copied, changed or removed without authorization during electronic data transfer or in the process of transmission or storage on data media, and that it is possible to review and establish where transmission of personal data is supported by data transfer facilities (transfer control),

- Guaranteeing that it can be reviewed and established retrospectively whether, and by whom, personal data has been entered, changed or removed from data processing systems (input control),

- Guaranteeing that personal data processed on behalf of the controller can only be processed in accordance with the controller's instructions (job control),

- Guaranteeing that personal data is protected against accidental destruction or loss (availability control),

- Guaranteeing that items of data collected for different purposes are processed separately (separation requirement).

- Providing possibility of pseudonymization and encryption of personal data.

- Providing ability to ensure confidentiality, integrity, availability and resilience of processing systems and services including ability to restore the availability and access to personal data.

- Providing a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

4.3 Data archiving

When data is archived, the principles of data processing, particularly with regard to data minimization and data avoidance, must be adhered to. Archiving personal data without the express consent of the data subject is forbidden unless this is necessary due to operational needs based on legal grounds. Section 2.1 applies with regard to the obligation for deletion.

5. Rights of the data subject

5.1 General obligations

(1) The controller shall take appropriate measures to provide information and communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form. The information shall be provided in writing, or by other means as appropriate.

(2) The controller shall provide information or action taken on a request under section 5.2 to the data subject without undue delay and in any event within one month of receipt of the request. Where necessary and on information of the data subject that period may be extended by two further months.

5.2 Right of Access

(1) Each data subject may demand confirmation as to whether personal data concerning him or her are being processed and where that is the case access to that data and information (including written information) on the data stored about him/her, including its origin, the purpose of storing the data, the recipients to which it has been disclosed and where possible the envisaged period for which the data will be stored or the criteria to determine that period. In addition, the data subject shall have access to information whether automate decision making, including profiling, exists, if so, about the logic involved and the significance and envisaged consequences of such processing. The data subject also shall have the right to be informed on appropriate safeguards relating to the transfer of personal data to a third country where applicable.

(2) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject the controller may impose a reasonable fee for issuing such information based on administrative costs.

5.3 Correction, restriction, erasure, right to be forgotten and data portability

(1) The data subject has the right to demand correction if the data stored about him/her is incomplete and/or incorrect.

(2) The data subject shall have the right to obtain from the controller restriction of processing under the reasons of Article 18 (1) GDPR when the accuracy of data is contested, the data subject requests the restriction of data no longer needed by the controller or where processing is unlawful or where the data subject has objected to processing according to section 5.4.

(3) Furthermore, he/she has the right to demand the deletion of his/her data if data processing was inadmissible or the data is no longer required for the data processing purpose or if any other reason mentioned in Article 17 (1) GDPR is applicable.
Where the controller has made the personal data public the controller, taking into account available technology and costs of implementation, shall take reasonable steps to inform controllers which are processing the personal data that the data subject has requested the erasure of by such controllers of any links to, or copy or replication of, those personal data (right to be forgotten). Above obligations do not apply where processing is necessary for compliance with legal obligations by Union or member State law which requires processing

(4) The data subject shall have the right to receive personal data concerning him or her which he or she has provided to a controller under the conditions in Article 20

GDPR in a structured, commonly used and machine-readable format (data portability).

5.4 Objection

(1) The data subject can object to the company responsible for using his/her data on grounds relating to his or her particular situation at any time to processing of personal data concerning him or her which is based on public interest, interest of official authority vested in the controller or based on legitimate interests pursued by the controller or by a third party. Unless the controller demonstrates compelling legitimate grounds for processing which override the interests of the data subject or for the establishment, exercise or defense of legal claims the controller shall no longer process the data.

(2) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing, which includes profiling to the extent that it is related to such direct marketing. In case of objection by the data subject the personal data shall no longer be processed for direct marketing purposes.

5.5 Discrimination Ban

Data subjects must not be discriminated against in any way if they exercise their rights.

5.6 Assertion

(1) The data subject may at any time contact the Data Protection Official of the company responsible and/ or the company with questions and/or complaints on the use of his/her personal data or with questions about the DHL Group Data Privacy Policy.

(2) In this context, “responsible” denotes all companies with which the data subject has a contractual relationship or at which his/her personal data is processed. The circumstance must be clarified in cooperation with the companies or divisions involved without culpable delay. The Data Protection Official of the company addressed will coordinate all relevant correspondence with the data subject.

(3) Notwithstanding the foregoing the data subject also has the right to lodge a complaint with a supervisory authority and/or to take legal action.

5.7 Copy of the DHL Group Data Privacy Policy

The Corporate Data Protection Officer will make available, upon request, a copy of the DHL Group Data Privacy Policy.

III. DATA PROTECTION MANAGEMENT

1. Corporate Data Protection Officer

(1) The Corporate Data Protection Officer coordinates cooperation and agreement on all matters concerning the DHL Group Data Privacy Policy. In particular, the Corporate Data Protection Officer is a representative to external parties and national/international data protection supervisory authorities in all matters concerning the content of the DHL Group Data Privacy Policy. The independence and freedom to give instructions of the Data Protection Officials appointed on the basis of the relevant national regulations will remain unaffected by this.

(2) The Corporate Data Protection Officer monitors the implementation of the DHL Group Data Privacy Policy on the basis of audits as well as other appropriate instruments and reports to the Group's Board of Management. Upon request, the Corporate Data Protection Officer will provide the Data Protection Authority with the relevant audit report. A relevant Data Protection Authority may ask the Corporate Data Protection Officer to conduct or let carry out - in line with applicable regulations - an audit in a Group company to verify compliance with DHL Group Data Privacy Policy. The group company in question must accept such an audit and adjust identified aspects of improvements.

(3) The Group companies are obliged to inform the Corporate Data Protection Officer if and when they accede to or withdraw from the DHL Group Data Privacy Policy. Yearly, and upon request, the Corporate Data Protection Officer will provide the Data Protection Authority with the list of acceded Group companies.

(4) The Corporate Data Protection Officer is also responsible for updating the DHL Group Data Privacy Policy. In the event of any changes, he/she must inform the Group Companies of the changes via the Data Protection Official in question and must obtain the consent of the Group Companies for amendments that are not mandatory by law or are not purely of an editorial nature. The Corporate Data Protection Officer will notify significant amendments to the Lead Data Protection Authority, which is the Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Federal Commissioner for Data Protection and Freedom of Information of Germany).

2. Data Protection/Privacy Steering Committee

In order to implement DHL Group Data Privacy Policy and to achieve continuous integration of Data Protection/Privacy into business processes, a Data Protection Steering Committee consisting of business divisions representatives, has been established. In particular, the Data Protection Steering Committee will support the

Corporate Data Protection Officer to establish and maintain a group-wide Data Protection Management

3. Data Protection Officials and Data Protection Advisors

(1) For each Group company, an independent Data Protection Official (Data Protection Officer / Data Protection Coordinator) must be appointed. The Data Protection Official is responsible for implementation of standards and regulations.

(2) In order to ensure compliance with the DHL Group Data Privacy Policy, Data Protection Officials must, in particular, be involved at an early stage in the development and design of new and altered operational processes, products/services and marketing measures. To enable these tasks to be performed, Group companies must inform relevant Data Protection Official of any relevant developments.

(3) Data Protection Advisors providing legal experience will support Data Protection Officials in fulfilling their tasks. In particular, as far as regulatory issues are concerned, Data Protection Officials should seek the advice of Data Protection Advisors.

(4) If there are no legal restrictions, the responsible Data Protection Official must be authorized to audit all processing methods locally which involve the use of personal data. To this end, they may – as far as they are in existence - use any Group-wide methods, for example joint data protection audits. A special audit program concerning the DHL Group Data Privacy Policy will be developed and has to be conducted by relevant Group companies. Upon request the Data Protection Official has to provide the Corporate Data Protection Officer with an audit report.

(5) The employees of Group companies must be trained adequately on the data protection regulations and the application of the DHL Group Data Privacy Policy.

4. Compliance

(1) Group companies must ensure the applicable national data protection provisions and the DHL Group Data Privacy Policy are adhered to.

(2) The Data Protection Official of the company in question must be informed of breaches (or suspicion of breaches) of data protection provisions and the DHL Group Data Privacy Policy without delay.

(3) In incidents that are relevant to more than one Group company, the Data Protection Official must also inform the Corporate Data Protection Officer and the competent Data Protection Advisor. They must also inform the Corporate Data Protection Officer if the laws applicable to a Group company change substantially in a disadvantageous manner and how this has effects on data protection or adherence to the DHL Group Data Privacy Policy.

(4) The Data Protection Officials and Advisors will mutually agree their activities under the DHL Group Data Privacy Policy, give each other support and use synergies. Together, they form part of the DHL Group Data Protection Network.

5. Cooperation with supervisory authorities

(1) The Group companies must ensure that they respond to requests from a Data Protection Authority within a reasonable period and to a reasonable extent. In line with applicable national legislation, they have to abide by the advice of a Data Protection Authority.

(2) The competent Data Protection Advisor shall be involved in handling of such requests.

IV. LIABILITY

1. Data transfer to a controller

(1) The data exporter and data importer shall each be individually liable to data subjects for material and non-material damages they cause by any breach of third-party rights under the DHL Group Data Privacy Policy. The liability of the data exporter under applicable national data protection law remains unaffected.

(2) The data exporter and data importer shall be liable to one another for damages they cause by any breach of the DHL Group Data Privacy Policy. Liability between the data exporter and the data importer is limited to actual damage suffered. For the avoidance of doubt the parties agree that they may be exempted from this liability if they prove that neither of them is responsible for the violation of those provisions.

(3) Punitive damages are specifically excluded.

(4) The data exporter and data importer entitle data subjects to enforce clauses as stipulated in section 3 against the data importer or the data exporter as a third-party beneficiary, for any of their respective breach of their contractual obligations, with regard to their personal data. Jurisdiction for this purpose is in the data exporter's country of establishment or jurisdiction of habitual residence of the data subject.

(5) In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly.

(6) A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the DHL Group Data Privacy Policy (the data exporter shall have the burden to prove that it took reasonable efforts).

2. Data transfer to a processor and/or sub-processor

(1) Any data subject, who has suffered damage as a result of any breach of the obligations referred to in section 3 by the data exporter, the data importer or the sub-processor, is entitled to receive compensation from the data exporter for the damage suffered.

(2) If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or their sub-processor of any of their obligations referred to in section 3, because the

data exporter has factually disappeared or ceases to exist in law or has become insolvent, the data importer entitles the data subject to issue a claim against them as if he was the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid their own liabilities.

(3) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in section 3 or chapter II section 2.7 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor entitles the data subject to issue a claim against him with regard to its own processing operations under the DHL Group Data Privacy Policy as if he was the data exporter or the data importer, unless any successor entity has assumed the entire obligations of the data exporter or the data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the DHL Group Data Privacy Policy.

(4) Jurisdiction for this purpose is in the data exporter's country of establishment.

3. Third party rights

Data subjects have the right to enforce as a third-party beneficiary, chapter II, III section 5 paragraph 1 and IV of the DHL Group Data Privacy Policy against the data exporter and/or – depending on the circumstances – the data importer or sub-processor for their respective breach of their obligations of the DP DHL Privacy Policy, with regard to their personal data.

4. Alternative dispute resolution

(1) Data subjects who believe that their right to protection of their individual sphere of life has been impaired by an actual or assumed act of processing their personal data may apply to the competent Data Protection Official of the respective group company, requesting arbitration. The Data Protection Official shall examine the legitimacy of the complaint and shall advise the data subject with regard to his/her rights. In so doing, the Data Protection Official is obliged to uphold the confidentiality of further personal data of which the Data Protection Official has been informed by the complainant, insofar as the latter does not release the Data Protection Official from this obligation. Upon the request of the data subject, the attempt may be made to reach a settlement of the complaint with the involvement of the data subject and

the Data Protection Official. Such a settlement may also include a recommendation concerning damages in connection with the infringement of the right to protection of their individual sphere of life.

(2) The right to make a complaint to the competent Data Protection Supervisory Authority and/or to take action remains unaffected by this provision.

V. ANNEX: DEFINITIONS

Anonymization
means changing personal data in such a way that individual details on personal and factual relationships cannot be attributed to a specific or specifiable natural person without a disproportionate amount of time, money and effort being required.

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 where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. The controller is not the legally dependent branch/business site of a legal person but rather the company as a whole; see Article 4 (7) GDPR.

Controller – processor agreement
An agreement as stipulated by Article 28 of the GDPR concerning the processing of personal data on behalf of the controller by a processor.

Data Exporter
is the group company established in a country of the European Union (EU) which transfers personal data to a Data Importer.

Data Importer
is the group company located in a third country which receives personal data from the data exporter.

Data processing
means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automatic 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; see Article 4 (2) GDPR.

Data Protection Official
may be - where provided by national laws – appointed as a statutory Data Protection Officer in accordance with such laws or in any other case appointed as a Data Protection Coordinator. If a Data Protection Coordinator is appointed at a Group company in addition to a statutory Data Protection Officer, the rights and obligations from the DHL Group Data Privacy Policy will be applied in data protection management by the Data Protection Officer, whereby this process will be supported by the Data Protection Coordinator in question.

Data subject
is every identified or identifiable natural person whose personal data is processed; see Article 4 (1) GDPR.

Data Transfer
means disclosure by transmission, e.g. passing on stored personal data, or personal data acquired through processing, to a third party by actively forwarding it or enabling third parties to retrieve it.

GDPR
General Data Protection Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free flow of movement of such data.

Group Company
means Deutsche Post AG, as well as all companies in which Deutsche Post AG has a direct or indirect stake of more than 50%, or over which it has financial control. Furthermore, in the context of the DHL Group Data Privacy Policy, companies which have voluntarily acceded to the DHL Group Data Privacy Policy are equalized with Group companies.

Onward transfer
Onward transfer exists if a data importer forwards data to other third parties that have their registered office in a third country or engages in the cross-border transfer of data.

Personal data
is 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; see Article 4 (1) GDPR.

Pseudonymization
is changing personal data using an allocation system, so that individual details can no longer be attributed to a natural person without knowledge or use of the allocation system.

Processor
means any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; see Article 4 (8) GDPR.

Profiling
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 analyze or predict aspects concerning that natural person's

performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Special categories of personal data
are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health or concerning a natural person's sex life or sexual orientation in the sense of Article 9 (1) GDPR.

Sub-processor
means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer, or from another sub-processor of the data importer, personal data exclusively intended for processing activities to be carried out on behalf of the data exporter in accordance with its instructions, the relevant terms of the DHL Group Data Privacy Policy and the terms of the written subcontract.

Third country
means any country outside European Union.

Third party
is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Bonn, 01-July-2023