DEUTSCHE POST DHL
DATA PRIVACY POLICY

Deutsche Post DHL

PREAMBLE

1. The use of modern information and communication technologies and the global networking of information flows are fundamental to the business processes of Deutsche Post DHL. Particularly, complex organisational structures and the challenge of being able to run the necessary applications on a 24-hour basis requires an international IT infrastructure in which personal data is processed on a group 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 Deutsche Post DHL.

2. The aim of this Deutsche Post DHL Data Privacy Policy is to establish a standardized, adequate and global data protection and data security standard for Deutsche Post DHL as a whole. In particular, the aim is to guarantee the 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.

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

TABLE OF CONTENTS

III. DATA PROTECTION MANAGEMENT

IV. LIABILITY

V. ANNEX: DEFINITIONS

I. SCOPE

1. Area of application

The Deutsche Post DHL 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 Economic Area to Group companies in a third country. The natures of the processed data, as well as the purposes of processing, depend on the relationship that individual data subjects may have with one or more Deutsche Post DHL Group companies. The information in question is mainly connected 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 variety of customer services.

The Deutsche Post DHL Data Privacy Policy does not apply to data transfers which are covered by derogations stipulated in Article 26 (1) of the EU Data Protection Directive, e.g. when a data subject has given his consent or when the transfer is necessary for the fulfillment of a contract. Also, the Deutsche Post DHL Data Privacy Policy does not apply to statistical analyses or studies performed on the basis of anonymised or pseudonymised data that do not allow conclusions to be made about data subjects.

2. Legally binding effect

The Deutsche Post DHL Data Privacy Policy will take effect upon authorization by the Group's Board of Management and upon publication.

The Deutsche Post DHL Data Privacy Policy will become binding for the individual Group companies by the commitment of the management of the companies in question to the observation of the regulations in a Declaration of Accession.

The binding effect will end upon revocation of the Deutsche Post DHL Data Privacy Policy or when the respective company withdraws from the Group.
In respect to the data transferred up to this time, the Group companies in question are obliged to observe the provisions contained in the Deutsche Post DHL Data Privacy Policy on handling personal data. Any further/future data transfers from and/or to Group companies may take place only when other adequate safeguards as stipulated by Article 26 of the EU Data Protection Directive are adduced.

3. Relationship to legal regulations

The principles of the Deutsche Post DHL Data Privacy Policy will not replace the necessary legitimization, under law if applicable, for the collection and processing of personal data, but they ensure compliance with specific requirements under the EU Data Protection Directive within the scope of cross-border data transfers to third countries. Hence, any (stricter) national regulation prevails over the requirements stipulated in this Privacy Policy.

Within the area of application of the EU Data Protection Directive, the permissibility of collecting, processing and using personal data is governed by the respective national and local laws. 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.

The admissibility of data processing and data use 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.

The admissibility of the collection, processing and transfer of personal data which have not been collected or processed within the scope of the said EU Data Protection Directive remains governed by the national laws of the relevant country of collection or processing.

Each Group company is responsible for checking the admissibility of data collection and 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.

Obligations and regulations for individual Group companies which relate to the processing and use of personal data and which go beyond the following principles, as well as containing further requirements for processing and using personal data, will not be affected by the Deutsche Post DHL Data Privacy Policy. Nevertheless, the companies agree that the laws applying to the individual companies will not prevent them from fulfilling their obligations as stipulated in the Deutsche Post DHL Data Privacy Policy.

The collection of personal data and/or its transfer to state offices will only take place in compliance with the relevant national regulations.

The Deutsche Post DHL Data Privacy Policy is subject to the laws of Germany in all other respects.

II. PRINCIPLES

1. Transparency of data processing

1.1 General duty to notify and inform
Data subjects must be suitably informed of how their personal data is handled. This shall also include the publication of the Deutsche Post DHL Data Privacy Policy on the Corporate Intranet

The duty to inform contains the following details:
- The identity of the office responsible for collecting and processing personal data, and its contact address (controller).
- The purpose and scope of data collection and processing.
- The nature of data processing, in particular if the data is to be processed or used abroad.
- If personal data is passed on to third parties, the names of those third parties as well as the reason why and to what extent the data is passed on to them.
- Rights of the data subject (section II, 5).

The information may be omitted if
- this is necessary in order to protect the data subject or the rights and freedoms of other persons,
- the data subject has already been informed,
- it would entail a disproportionate expense,
- the data is accessible to the public and information would be disproportionately extensive due to the high number of cases involved.

The information must be made available to the data subject the first time data is collected and as required thereafter.

1.2 Special duties to inform
If the data subject is contacted for advertising or market/opinion research purposes, the first time contact is made they must also be notified of their right to object to their data being used or transferred for direct marketing purposes. In particular, this must include suitable information on exercising their right to object, including information on the office to which their objection may be submitted.

2. General admissibility requirements for the collection, processing and use of data

2.1 Principle of legitimating basis
Personal data may only be collected, processed and used if such actions are legally admissible or if the data subject has given their 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 business 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 collecting, processing and using personal data which is required. Taking account of the intended purpose for using personal data, the data must be appropriate and relevant and may 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 with a disproportionate amount of effort.

2.4 Purpose limitation
Personal data may only be collected and processed for specific, clear and lawful 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 or if permitted by the national law of the data exporter.

2.5 Consent
If the collection, processing or use of personal data is not required for the purpose of initiating or fulfilling a contract or there is no other legal permission, the consent of the data subject must be obtained no later than the date on which the collection, processing or use of personal data begins.

The consent must be given expressly and voluntarily and on an informed basis, which clearly shows the extent of the consent and the possible consequences of withholding consent for 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.

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 their consent to the use of their 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
If a Group company accepts a commission to process 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, 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.

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

If agreements are concluded with processors and/or sub-processors in countries without an adequate data protection standard and which do not fall under the scope of this Privacy Policy, adequate safeguards as stipulated by Article 26 of the EU Data Protection Directive 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
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 which provide for adequate safeguards as stipulated by Article 26 of the EU Data Protection Directive must be agreed upon with the recipient. These measures will also apply in the case of any further onward transfer.

If personal data which has been processed under the scope of the EU Data Protection Directive is transferred to offices which are not subject to the Deutsche Post DHL Data Privacy Policy or to third parties in third countries without an adequate level of protection, adequate safeguards as stipulated by Article 26 of the EU Data Protection Directive must be adduced. Notwithstanding the foregoing, personal data may only be transferred within the framework of the EU Data Protection Directive or within the framework of the national regulations passed on the basis of the EU Data Protection Directive.

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.

3. Special data processing cases

3.1 Special categories of personal data
The collection, processing and use of special categories of personal data is forbidden unless the collection, processing and use of such data is necessary and the data subject expressly consents to it. In addition, special personal data may only be collected, processed and used within the framework of the exceptions specified in the EU Data Protection Directive or within the framework of the national exception regulations passed on the basis of the EU Data Protection Directive.

Before such collection, processing or use 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
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 automatic processing. These include, in particular, decisions for which data on the credit worthiness, professional performance or health of the data subject is applicable.

If, in individual cases, it is objectively necessary to make automated decisions, the data subject must be informed of 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.

3.3 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 use of his/her data for this purpose and must be informed separately of this as per section II, 1.2. If the data subject objects, the data must be blocked for this purpose.

4. Data quality/data security

4.1 Confidentiality of data processing
Only authorized employees especially charged with the observance of data protection may collect, process or use personal data. It is forbidden for an employee to use 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
If personal data is processed or used, suitable technical and organizational measures must be taken to protect the company processes and IT systems, in order to protect personal data against unintentional or unlawful deletion, alteration, communication, access or loss.

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).

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 for operation based on legal grounds. section II, 2.1 applies with regard to the obligation for deletion.

5. Rights of the data subject

5.1 Information
Each data subject may demand information (including written information) on the data stored about him/her, including its origin, the purpose of storing the data and the persons and offices to which it has been communicated. However, such a claim will not exist if the interest in maintaining the business secret outweighs the interest of the data subject.

The information must be given to the data subject in a clearly understandable form within an appropriate period of time. The companies may impose a fee for issuing such information if permitted under the law of the country in question.

5.2 Correction, blocking, deletion, objection
The data subject has the right to demand correction if the data stored about him/her is incomplete and/or incorrect.

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 purpose of data processing. If there are legal storage periods or deletion is not possible or reasonable, the data will be blocked instead of deleted.

The data subject can object to the use of his/her data by the company responsible if he/she has a contractual or statutory right to object. The right to object also applies in cases in which the data subject gave his/her consent to the use of his/her data previously.

5.3 Discrimination ban
Data subjects may not be discriminated against in any way if they exercise their rights.

5.4 Assertion
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 about the use of his/her personal data or with questions about the Deutsche Post DHL Data Privacy Policy.

In this context, "responsible" denotes all companies with which the data subject has a contractual relationship or by 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.

5.5 Copy of the Deutsche Post DHL Data Privacy Policy
The Corporate Data Protection Officer will make available, upon request, a copy of the Deutsche Post DHL Data Privacy Policy.

III. DATA PROTECTION MANAGEMENT

1. Corporate Data Protection Officer

The Corporate Data Protection Officer coordinates cooperation and agreement on all matters concerning the Deutsche Post DHL 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 Deutsche Post DHL Data Privacy Policy. The independence of the appointed Data Protection Officials and their freedom to give instructions on the basis of the relevant national regulations will remain unaffected by this.

The Corporate Data Protection Officer monitors the implementation of the Deutsche Post DHL 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 an audit or arrange for an audit to be carried out – in line with applicable regulations – in a Group company to verify compliance with Deutsche Post DHL Data Privacy Policy. The Group company in question must accept such an audit and adjust identified aspects of improvements.

The Group companies are obliged to inform the Corporate Data Protection Officer if and when they accede to or withdraw from the Deutsche Post DHL 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.

The Corporate Data Protection Officer is also responsible for updating the Deutsche Post DHL 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 the Lead Data Protection Authority, which is the Federal Commissioner for Data Protection and Freedom of Information of Germany, of significant amendments.

2. Data Protection/Privacy Steering Committee

In order to implement the Deutsche Post DHL Data Privacy Policy and to achieve continuous integration of Data Protection/Privacy in business processes, a Data Protection Steering Committee consisting of business division representatives has been established. In particular, the Data Protection Steering Committee will support the Corporate Data Protection Officer to establish and maintain group-wide Data Protection Management.

3. Data Protection Officials and Data Protection Advisors

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.

In order to ensure compliance with the Deutsche Post DHL 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. In order to make this possible, Group companies must inform the appropriate Data Protection Official of any relevant developments.

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.

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 place – use any group-wide methods, for example joint data protection audits. A special audit program concerning the Deutsche Post DHL 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.

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

4. Compliance

Group companies must ensure that the applicable national data protection provisions and the Deutsche Post DHL Data Privacy Policy are adhered to.

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

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 responsible 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 effects data protection or adherence to the Deutsche Post DHL Data Privacy Policy.

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

5. Cooperation with supervisory authorities

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 comply with the advice of a Data Protection Authority.
The responsible Data Protection Advisor shall be involved in handling such requests.

IV. LIABILITY

1. Data transfer to a controller

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

The data exporter and data importer shall be liable to one another for damages they cause by any breach of the Deutsche Post DHL Data Privacy Policy. Liability between the data exporter and the data importer is limited to actual damage suffered. For the prevention of any 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.

Punitive damages and non pecuniary damages are specifically excluded.

The data exporter and data importer entitle data subjects to enforce clauses as stipulated in Article 3 of this Section against the data importer or the data exporter as a third party beneficiary, for any of their respective breaches of their contractual obligations, with regard to their personal data. Jurisdiction for this purpose is in the data exporter's country of establishment.

In cases involving allegations of breaches by the data importer, the data subject must first request that the data exporter 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.

A data subject is entitled to proceed directly against a data exporter which has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under the Deutsche Post DHL 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

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

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 its sub-processor of any of their obligations referred to in Article 3 of this Section, 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 it as if it were 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 an entity.

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

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 its obligations referred to in Article 3 or in Article 2.7 of Section II 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 Deutsche Post DHL Data Privacy Policy as if he were 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 an entity. The liability of the sub-processor shall be limited to its own processing operations under the Deutsche Post DHL Data Privacy Policy.

Jurisdiction for this purpose is in the controller's country of establishment.

3. Third party rights

Data subjects have the right to enforce as a third party beneficiary, section II, III, 5 paragraph 1 and IV of the Deutsche Post DHL 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 Deutsche Post DHL Data Privacy Policy, with regard to their personal data.

4. Alternative dispute resolution

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 responsible 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 doing so, the Data Protection Official is obliged to uphold the confidentiality of further personal data which the Data Protection Official has been informed of 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.

The right to make a complaint to the responsible 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 which alone, or jointly with others, determines the purposes and means of the processing of personal data. The controller is not the legally dependent branch/business site of a legal person but rather the company as a whole.

Controller – processor agreement
An agreement as stipulated by Article 17 of the EU Data Protection Directive concerning the processing of personal data on behalf of the controller by a processor.

Data collection
is the procurement of data on the data subject.

Data exporter
is the Group company established in a country of the European Economic Area (EEA) 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 upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

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 Deutsche Post DHL 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 collected, processed or used.

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.

Data use
means e.g. the use of personal data, unless it already constitutes data processing.

EU Data Protection Directive
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 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 Deutsche Post DHL Data Privacy Policy, companies which have voluntarily acceded to the Deutsche Post DHL Data Privacy Policy are made equal with 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 person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific of their physical, physiological, mental, economic, cultural or social identity.

Pseudonymization
is changing personal data by 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 established in a third country which processes personal data on behalf of the controller.

Special categories of personal data
are information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life in the sense of Article 8 (1) of the EU Data Protection Directive.

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 Deutsche Post DHL Data Privacy Policy and the terms of the written subcontract.

Third country
means any country outside the scope of the EU Data Protection Directive.

Third party
is any person or organization other than the controller. Third parties are not the data subjects themselves or individuals or organizations which, under the direct authority of the controller or processor, are authorized to process the data.

Publisher:
Deutsche Post AG
Corporate Center
Corporate Communication / Internal Kommunikation
Responsible:
Corporate Data Protection Officer
53250 Bonn

Status: August 2012

Deutsche Post DHL