Data Processing Agreement

1. General Information

The regulations in this data processing agreement concluded between Deutsche Post AG – hereinafter referred to as the "Processor" – and its customers – hereinafter referred to as the "Controller" – apply to the management of personal data in the DHL business customer portal beyond the data processing required for the provision of postal services.

2. Subject Matter of the Data Processing

The Processor shall provide the Controller with the additional "Track Letter" function – which is not necessary for the provision of postal services – for tracking shipments with the DHL business customer portal. This function provides the customer with an overview of the shipments sent with DPAG, including the recipient details, the current shipment status and the shipping process.

3. Duration

This data processing agreement is tied to the term of the Main Agreement.

4. Description of the Processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the Controller, are provided in Annex I.

5. Obligations of the Parties

1. Instructions
   a. The Processor shall process personal data only upon the documented instruction of the Controller, unless it is obligated to process data under Union law or under the law of a Member State to which it is subject. In such a case, the Processor shall inform the Controller of these legal requirements prior to processing, unless the law in question prohibits this on important grounds of public interest. The Controller may issue further instructions throughout the processing of personal data. These instructions shall always be documented. Since the "Track Letter" function is a standardized service for a large number of customers, the Processor reserves the right to terminate the contract for the provision and use of the "Track Letter" service from Deutsche Post AG without notice if the instructions of the Controller cannot be followed within the framework of the standardized process.
   b. The Processor shall inform the Controller immediately if it believes that instructions issued by the latter are in contravention of Regulation (EU) 2016/679 or applicable data protection provisions of the Union or Member States.
2. Purpose limitation

The Processor shall process the personal data only for the specific purpose(s) stated in Annex I unless it receives additional instructions from the Controller.

3. Security of processing
   a. The Processor shall take at least the technical and organizational measures listed in Annex II to ensure the security of the personal data. This includes protecting the data from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the data (hereinafter referred to as "personal data breach"). In assessing the appropriate level of protection, the parties shall take due account of the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing, as well as the risks involved for the data subjects.
   b. The Processor shall grant its personnel access to the personal data that is subject to processing only to the extent strictly necessary for the performance, management and supervision of the agreement. The Processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
4. Documentation and compliance with the clauses
   a. The parties must be able to demonstrate that they have complied with these clauses.
   b. The Processor shall promptly and appropriately handle requests from the Controller regarding the processing of data pursuant to these clauses.
   c. The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set forth in these clauses and arising directly from Regulation (EU) 2016/679. At the request of the Controller, the Processor shall also permit an audit of the processing activities covered by these clauses if
      – the Controller has reason to assume that the Processor is not acting in compliance with the technical/organizational measures and/or the obligations under this agreement;
      – a security breach has occurred;
      – the regulatory authority responsible for the Controller requests such an audit.

   When deciding on a review or audit, the Controller may consider relevant certifications of the Processor.
   d. Notwithstanding the foregoing, evidence of compliance with the applicable requirements can be furnished in the following ways:
      – Compliance with the approved codes of conduct and/or

- Certification under an approved certification procedure in accordance with Article 42 of the GDPR and/or
- recent certificates issued by auditors, reports or excerpts from reports provided by independent bodies. At 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 may reasonably verify whether the Processor is implementing the technical and organizational measures and fulfilling the obligations under this agreement.

e. The Controller may conduct the audit itself or instruct an independent auditor to do so. Audits may include inspections of the Processor's premises or physical facilities and shall be conducted with reasonable advance notice, as appropriate. If the Controller conducts an audit at the Processor's premises or facilities, this shall be done under the following conditions:
   - after prior notice of at least ten (10) working days;
   - audits shall be conducted only during standard business hours and not more than once a year;
   - the audit shall be limited to the data that are relevant to the Controller;
   - the Controller shall prevent any disruption to the normal business operations of the Processor;
   - the Controller shall ensure, where legally permissible, the confidentiality of all collected information that is to be kept confidential owing to its nature.
   - Each party shall bear the costs incurred by it. If the audit imposes work/outlay on the Processor or another processor that exceeds one business day, the Controller agrees to reimburse all costs related to additional days.

f. Upon request, the parties shall make available to the appropriate regulatory agency or agencies the information specified in this clause, including the results of audits.

5. Use of Subcontracted Processors

   a. The Processor has the general authorization of the Controller to engage sub-processors. A list of sub-processors is provided in Annex III. The Processor shall explicitly inform the Controller in writing at least four (4) weeks in advance of any intended changes to this list in the form of addition or removal of sub-processors, and shall allow the Controller sufficient time to object to these changes before the sub-processor(s) in question is/are commissioned. The Processor shall provide the Controller with the necessary information to enable the Controller to exercise its right to object. A list of sub-processors is provided in Annex III. The parties shall ensure that Annex III is kept up to date.

   b. Where the Processor instructs a sub-processor to perform certain processing activities (on behalf of the Controller), this instruction shall take the form of a contract that binds the sub-processor to essentially the same data protection obligations as those that apply to the Processor in accordance with these clauses. The Processor shall ensure that the sub-processor meets the obligations that are imposed on the Processor in accordance with these clauses and Regulation (EU) 2016/679.

   c. The Processor shall provide the Controller with a copy of any such subcontracting agreement and any subsequent amendments upon the Controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the Processor may obscure the wording of the agreement prior to disclosing any copy.

   d. The Processor shall be fully liable to the Controller for the sub-processor's compliance with its obligations under the contract concluded with the Processor. The Processor shall notify the Controller if the sub-processor fails to fulfil its contractual obligations.

6. International data transfers

   a. Any transfer of data by the Processor to a third country or an international organization shall take place exclusively on the basis of documented instructions from the Controller or to comply with a specific provision under Union law or the law of a Member State to which the Processor is subject, and must be in accordance with Chapter V of Regulation (EU) 2016/679.

   b. The Controller agrees that where the Processor uses a sub-processor pursuant to Clause 7.7 to carry out certain processing activities (on behalf of the Controller) and such processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46 (2) of Regulation (EU) 2016/679, provided that the conditions for the application of those standard contractual clauses are met.

6. Support for the Controller

1. The Processor shall immediately inform the Controller of any request received from the data subject. It shall not answer the request itself, unless it has been authorized to do so by the person in charge.
2. Taking into account the nature of the processing, the Processor shall assist the Controller in fulfilling the latter's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations according to letters a) and b), the Processor shall follow the instructions of the Controller.
3. Aside from the Processor's obligation to assist the Controller pursuant to Clause 6 (b), the Processor, taking into account the nature of the data processing and the information available to it, shall also assist the Controller in complying with the following obligations:

   a. The obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (hereinafter referred to as "data protection impact assessment"), if a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;

b. The obligation to consult the responsible supervisory authority/authorities prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

c. The obligation to ensure that the personal data are factually correct and up to date, in that the Processor shall inform the Controller without delay if it discovers that personal data processed by it are incorrect or out of date;

d. Obligations arising from Article 32 of Regulation (EU) 2016/679.

4. In Annex II, the parties set out the suitable technical and organizational measures for the Processor's support of the Controller in the application of this clause, as well as the scope and applicability of the required support.

7. Notification of Personal Data Breaches

In the event of a personal data breach, the Processor shall work with the Controller and shall support the latter accordingly so that the Controller may meet its obligations under Articles 33 and 34 of Regulation (EU) 2016/679, with the Processor taking into account the nature of the processing and the information available to it.

1. Breach of data processed by the Controller

In the event of a personal data breach that concerns the data processed by the Controller, the Processor shall support the Controller as follows:

a. in the immediate reporting of the personal data breach to the responsible supervisory authority/authorities, after the Controller has become aware of the breach, where relevant (unless the personal data breach is unlikely to result in a risk to the personal rights and freedoms of natural persons);

b. in the collection of the following information, which is to be provided in accordance with Article 33 (3) of Regulation (EU) 2016/679 in the Controller's report, this information being required to include at least the following:
   - the nature of the personal data including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   - the likely consequences of the personal data breach;
   - the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If and to the extent that all such information cannot be provided at the same time, the original report shall contain the information available at that time, and further information shall be provided subsequently as soon as it is available without undue delay;

c. in compliance with the obligation arising from Article 34 of Regulation (EU) 2016/679 to inform the data subject of the data breach without undue delay if this breach is likely to result in a high risk to the rights and freedoms of natural persons.

2. Breach of data processed by the Processor

In the event of a personal data breach that concerns the data processed by the Processor, the Processor shall report this breach to the Controller without delay after it has become aware of the breach. This report must include at least the following information:

a. a description of the nature of the breach (where possible, stating the categories and approximate number of data subjects concerned and the approximate number of data records concerned);

b. details of a point of contact from which further information about the personal data breach can be obtained;

c. the expected consequences and the measures taken or proposed to be taken to address the personal data breach, including measures to mitigate its possible adverse affects.

If and to the extent that all such information cannot be provided at the same time, the original report shall contain the information available at that time, and further information shall be provided subsequently as soon as it is available without undue delay.

The parties shall set out in Annex II any other information that the Processor is required to provide in order to assist the Controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

8. Violations of the Clauses and Termination of the Agreement

1. If the Processor fails to comply with its obligations under these clauses, the Controller may – without prejudice to the provisions of Regulation (EU) 2016/679 – instruct the Processor to cease processing personal data until it is in compliance with these clauses or the agreement is terminated. The Processor shall inform the Controller immediately if it is unable to comply with these clauses for any reason whatsoever.

2. The Controller is entitled to terminate the agreement insofar as it relates to the processing of personal data in accordance with these clauses if

a. the Controller has suspended the processing of personal data by the Processor pursuant to point (a) and compliance with these clauses has not been re-established within an appropriate period of time, and in any case within one month following the suspension;

b. the Processor materially or persistently breaches these clauses or fails to meet its obligations under Regulation (EU) 2016/679;

c. the Processor does not comply with a binding decision of a competent court or the responsible supervisory authority/authorities concerning its obligations under these clauses, Regulation (EU) 2016/679.

3. The Processor is entitled to terminate the agreement insofar as it relates to the processing of personal data in accordance with these clauses if the Controller insists on the fulfillment of its instructions after having been informed by the Processor that its instructions violate applicable legal requirements pursuant to Clause 7.1 (b).
4. Upon termination of the contract, the Processor shall, at the choice of the Controller, erase all personal data processed on behalf of the Controller and shall warrant to the Controller that this has been done, or it shall return all personal data to the Controller and erase any copies, unless Union or Member State law requires storage of the personal data. The Processor shall continue to guarantee compliance with these clauses until the data have been erased or returned.

I. ANNEX – DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data are processed:
Customers of DPDHL customers (recipients)

Categories of personal data that are processed:
Shipment details (recipient's name and address)

II. ANNEX – TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING MEASURES FOR ENSURING DATA PROTECTION

1. Monitoring physical access to premises (access control)

Unauthorized persons must not be allowed to access data processing systems with which personal data are processed or used.

Implemented?	Measure	Comment
Yes	1. Definition of authorized persons (company employees and third parties)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	2. Binding process for the granting and transfer of access authorizations	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	3. Authorization IDs	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	4. Rules for keys	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE For each data center, rules for locking and keys must be established that govern the issuing of keys, access cards and number combinations. These rules must also encompass local regulations for exceptional cases (e.g., absence of the key holder, maintenance work outside business hours or false alarms).
Yes	5. Rules for third parties	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	6. Attendance records	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE In order to ensure that only authorized personnel are granted access, security areas must be protected by suitable access controls. A procedure for managing key issuance, access cards and number combinations must be documented for every data center. Every site must define rules for special cases, such as the absence of the key holder, maintenance work outside business hours or false alarms.
Yes	7. Visitor IDs	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Visitors to data centers must authenticate themselves. Upon receipt of a photo ID (e.g., valid driver's license or passport), they will be issued a visitor ID.
Yes	8. Guidelines for accompanying visitors	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Visitors must not be left unaccompanied at any time. It must be ensured that all visitors leave the data center before the end of the working day and return their visitor ID.
Yes	9. Security also outside of working hours via alarm system and/or plant security	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE In order to protect areas that contain confidential information, information that is important to the business, or information processing apparatus, security zones must be defined and used.

Implemented?	Measure	Comment
Yes	10. Create security areas and few access routes	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE In order to protect areas that contain confidential information, information that is important to the business, or information processing apparatus, security zones must be defined and used. IT systems for information processing must be protected by physical security boundaries against unauthorized access. Network components must be installed in building services rooms on site, in offices, or in secured cabinets. Servers must be located in site-specific or office-specific building services rooms, or in regional/domestic data centers.
Yes	11. Access to security areas must be logged and access routes restricted (including the ability to evaluate log files if needed)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Physical access by staff from external companies to rooms that contain DPDHL infrastructure (e.g., data centers and building services rooms at the site/company headquarters) must be documented in a logbook. Management of this logbook is the duty of the responsible business division. Elements to be documented include the following: a) Name and company b) Time of access and exit time c) Reason for work d) Affected IT devices or systems e) Signature of the external staff member f) Supervisor within the DPDHL division
Yes	12. Secured entrance for incoming and outgoing deliveries	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Access points such as delivery and loading zones, as well as other zones via which unauthorized persons could gain access to company buildings must be monitored and, where possible, isolated from information processing apparatus, in order to prevent unauthorized access.
Yes	13. Door security at emergency exits and other entrances and exits (electric door closing mechanism, identity card reader, television monitor, gatekeeper)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE IT systems for information processing must be protected by physical security boundaries against unauthorized access. Network components must be installed in building services rooms on site, in offices, or in secured cabinets. Servers must be located in site-specific or office-specific building services rooms, or in regional/domestic data centers.
Yes	14. Installation of locks	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE In order to protect areas that contain confidential information, information that is important to the business, or information processing apparatus, security zones must be defined and used.
Yes	15. Closed-shop operations	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE In order to protect areas that contain confidential information, information that is important to the business, or information processing apparatus, security zones must be defined and used.

Implemented?	Measure	Comment
Yes	16. Mutual monitoring (4-eye principle)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Data protection, accuracy and consistency are of particular importance in relation to firewalls. Current data stores of all software, rules and log files must be available and their recoverability must be tested. In order to avoid information security or operational risk from importing data or inconsistent, out-of-date storage versions (e.g., firewall rules), effective procedures for testing for consistency and validity, as well as emergency procedures, must be defined and used. Operational activities on firewalls that are critical to information security must be performed in compliance with the 4-eye principle.
Yes	17. Appropriate measures for securing the premises (e.g., special glazing, burglar alarm system, protection of shafts, site surveillance)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	18. Additional security measures in the data center (e.g., cages or lockable racks)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE

2. Monitoring access to data processing systems (access control)

Measures must be taken to prevent the possibility of data processing systems being used by unauthorized persons

Implemented?	Measure	Comment
Yes	1. Encryption	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	2. Identification of a terminal and/or the user of a terminal relative to the data processing system (e.g., using ID card readers)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	3. Allocation and protection of identification keys	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	4. Allocation of individual terminals and identification characteristics solely for certain functions	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	5. Functional and/or time-based restriction of terminal use and identification characteristics	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	6. User authorization rules	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	7. Undertaking to maintain data confidentiality	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE When adjusting and amending existing contracts, employees must be required to maintain confidentiality with regard to knowledge gained in the course of their professional activities, as well as to comply with the specifications and legal requirements summarized in the Information Security Policy.
Yes	8. Utilization of user codes for data and programs	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	9. Use of encryption routines for files	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	10. Differentiated access controls (e.g., by means of segment access locks)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	11. File organization guidelines	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	12. Logging and analysis of file usage	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	13. Special control of the use of auxiliary programs that could potentially circumvent the security measures	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	14. Monitored destruction of data media	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE

Yes	15. Work instructions and processing methods for data entry templates	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	16. Testing, coordination and monitoring systems	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	17. Program checking and approval processes	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	18. Deletion or disabling of user rights after the end of a contract	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE General changeover and termination measures (extension of the ISO standard) All erasure of authorizations must be traceably documented when an employee leaves the organization.
Yes	19. Network separation for greater safeguarding of access opportunities	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Groups of information services, users and information systems should be kept separately from one another in networks.
Yes	20. External access to the internal network only possible via an encrypted VPN (virtual private network) connection	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE With regard to security-related aspects, the following requirements for remote workplaces must be enforced: Encryption of communications and use of virtual private networks (VPNs).
Yes	21. Intrusion Detection System (IDS)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	22. Intrusion Prevention System (IPS)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	23. Mobile Device Management System	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	24. Security measures for log files	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	25. Remote access logging (option to analyze log files if necessary)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	26. Regular review of user accounts for validity and deactivation (after a specified time period)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Asset owners must review the access rights of all accounts as follows and modify them as needed: a) Personal accounts and non-personal accounts at least every twelve months; b) Administrator accounts and privileged accounts at least every six months. Asset owners must also check the access rights and modify them as applicable if the account owner changes, e.g., in the event of promotion, demotion, change of role, function, department of corporate division, or if the employment relationship is ended.

3. Monitoring data access (access controls)

It must be ensured that the persons authorized to use a data processing system can access only the data covered by their access authorization and that Personal Data cannot be read, copied, changed or erased during processing, use and after storage without proper authorization.

Implemented?	Measure	Comment
Yes	1. Encryption	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	2. Data station with function authorization key	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	3. Access authorization rules (e.g., user groups)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	4. Verification of authorization, automated, e.g., via identification key	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	5. Recording user access (e.g., program execution, writing, reading, erasing, breaches)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	6. Analysis of log files	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Not applicable (no terminals)	7. ID reader at the terminal	Not relevant
Yes	8. Time-restricted access	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	9. Partial access to databases and functions	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Not applicable (no data archiving)	10. Access-protected data archiving	Not relevant
Yes	11. Clear desk/clear screen policy	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE A clear desk policy for documents and mobile storage devices and a clean screen policy for information processing apparatus must be implemented.

Implemented?	Measure	Comment
Yes	12. Limited number of administrator accounts	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE For availability reasons, (preferably) two or more administrators should be assigned to system management for highly critical applications.
Yes	13. Automatic logout or screen locking after a period of inactivity	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Clear screen policies a) Screensavers should be activated manually as soon as a user temporarily leaves their workplace unsupervised b) After an appropriate period of inactivity, screen contents should be hidden and the keyboard locked automatically
Yes	14. Monitoring and/or regular control of activities by users with extensive access rights (e.g., super users, administrators)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE For user accounts with a high degree of authorization, the following additional measures must be taken: a) dministrators may use their administrator accounts for administration activities only and not for other activities (e.g., e-mail, surfing the internet); b) ll administrator activities must be logged; c) ll administrator accounts must be assigned to a single, identifiable person. Shared or group administrator accounts are not permitted; d) If administrators need to complete certain tasks using a system account with a high authorization level (e.g., root), and if such a possibility exists in the system, administrators must first log in with their non-privileged account and perform a traceable user change to the administrator account (e.g., “su” and/or “sudo” in UNIX) before they perform tasks with administration rights; e) Access to access-restricted and/or confidential areas must be restricted to the file, directory, or IP level; f) For availability reasons, (preferably) two or more administrators should be assigned to system management for highly critical applications. If only one administrator has been defined for system management of these applications, suitable recover measures must be put in place so that the (administrator) password can be restored in a secure and controlled manner.
Yes	15. Separation of authorization approval and authorization allocation (different functions)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Protection of external identities, customer data, employee data, and data from business partners (extension of the ISO standard) Identities and customer data, employee data, and partner data are special types of information that require additional protection.
Yes	16. Four-eyes principle when granting authorization to particularly sensitive data	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	17. Concept for allocation of and role management for access authorization of users (in particular super users/administrators)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE A formal log-in and log-out process for accounts must be implemented so that the account owner can be assigned, and access rights can be allocated and removed.

Implemented?	Measure	Comment
Yes	18. IT security concept including specific provisions for allocating rights (“need to know”, “need to have” principles)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE A security concept must be created and managed. Before a new service is selected from an external service provider, a process for managing information security risks must be carried out. A formal log-in and log-out process for accounts must be implemented so that the account owner can be assigned, and access rights can be allocated and removed. Accounts must be given access rights that are necessary for fulfilling their tasks according to the principle of least privileges, the need-to-know principle, and the separation of tasks.
Yes	19. Process for logging and reporting authorization changes (relocations)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Every allocation of account rights must be identifiable in the IT system and the circumstances must be recorded such that they can be traced at any time if requested. The following information must be traceable: a) first name and surname of the account owner; b) account ID; c) account ID of the person who grants access to the account; d) functional justification; e) access rights granted.

4. Transfer control

It must be ensured that personal data cannot be read, copied, changed or removed by unauthorized persons during electronic transmission, transport or storage on data media and that there are options for checking and determining at which points transfers of Personal Data using data transmission facilities are possible.

Implemented?	Measure	Comment
Yes	1. Implementation and use of encryption standards that correspond to the latest state of the art (based on the specific risk and the required level of protection)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	2. Definition of authorized persons	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	3. Mutual monitoring (4-eye principle)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	4. Secured entrance to data center for incoming and outgoing deliveries	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Delivery and loading zones Measure Access points such as delivery and loading zones, as well as other zones via which unauthorized persons could gain access to company buildings must be monitored and, where possible, isolated from information processing apparatus, in order to prevent unauthorized access.
Yes	5. Logging data transfers (and analysis if necessary)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	6. Protection against unauthorized mass data transfer	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE

Implemented?	Measure	Comment
No applicable (data media not issued)	7. Provision of data media solely to authorized persons (e.g., order confirmation, paperwork)	Not relevant
Yes	8. Data media management	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Not applicable (no fixed disk storage)	9. Fixed disk storage	Not relevant
Yes	10. Inventory control	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Not applicable (data media not issued/removed)	11. Separate sealing of confidential data media	Not relevant
Not applicable (data media not issued/removed)	12. Safety cabinets	Not relevant
Yes	13. Ban on taking bags and any other luggage into the secured areas	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	14. Monitored destruction of data media (e.g., misprints)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	15. Photocopying rules	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	16. Documentation of the access and transmission programs	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	17. Documentation of the units to which data are to be transmitted as well as the transmission channels (configuration)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	18. Specific authorized users	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Not applicable (data media not issued/removed)	19. Packaging and shipping rules (type of dispatch e.g., in sealed containers)	Not relevant
Not applicable (data media not issued/removed)	20. Direct collection, courier service, accompanied transportation	Not relevant
Yes	21. Plausibility check	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	22. Check for any errors or omissions	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Not applicable (no exchange of physical data media/ cloud)	23. Remaining data erased prior to exchange of data media	Not relevant
Not applicable (EU/EEA only)	24. Performance of a data transfer impact assessment (DTIA) if transferring data to non-EU/EEA countries and/or countries without a valid adequacy decision	Not relevant
Not applicable (EU/EEA only)	25. Definition and review of minimum requirements with regard to the data protection level when processing data in non-EU/EEA countries and/or countries without a valid adequacy decision	Not relevant

5. Input control

It must be possible to check and determine retrospectively whether personal data has been entered, changed or erased in data processing systems and, if so, by whom.

Implemented?	Measure	Comment
Yes	1. Evidence of organizationally defined responsibilities respecting data entry	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE The following controls must be implemented: a) Existing review mechanisms in standard applications should be activated (e.g., SAP) b) Application of the double review principle for critical data entry c) Definition of roles, responsibilities, and processes as part of the data entry process d) Technical measures for detecting attacks and alerts in the event of unauthorized data entry on a website (e.g., cross-site scripting, SQL injection) for critical IT applications
Yes	2. Data entry logs	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	3. File usage logs	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	4. Process, program and workflow organization	Process, program and workflow organization are implemented in accordance with internal project procedure methods.
Yes	5. Undertaking to maintain data confidentiality	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Confidentiality agreements must comply with the relevant legislation and requirements for such agreements, be reviewed regularly and renewed whenever necessary.
Yes	6. Evaluation of log files for particular incidents	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	7. Monitoring the correctness of entered data	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Based on the classifications of information processed and business requirements, measures must be incorporated into applications to ensure accuracy in processing, validate data entry and prevent errors, data loss and unauthorized modification or misuse of data.
Yes	8. Logging of data protection-relevant activities performed by administrators	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	9. Observance of the principle of data economy through process design, technical measures or by limiting the collection of personal data	DHL GROUP CORPORATE DATA PROTECTION POLICY Data processing shall be guided by the objective of processing only the necessary personal data. Personal data must be appropriate and relevant, taking into account the purpose for which it is to be used, and must not exceed the necessary scope (data economy). Personal data may only be processed within the scope of a specific application if this is necessary (data avoidance).

6. Obligations and monitoring of subcontracted processors (sub-processor contracts).

The Processor must ensure that the data processed on behalf of third parties are processed strictly in accordance with the instructions of the Controller. In all cases, once the sub-processing has been approved by the Controller, the Processor shall legally oblige third parties to comply with appropriate TOMs that are comparable and at least equivalent to its own obligations.

Implemented?	Measure	Comment

Yes	1. Engaging sub-processors exclusively on the basis of a data protection agreement pursuant to Article 28 GDPR	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	2. Comprehensive review of the TOMs warranted by the subcontractor before and periodically during the processing	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Not applicable	3. Review and assessment of the level of data protection in non-EU/EEA countries (if applicable)	Not relevant
Yes	4. Request and approval of declarations and guarantees to obligate all subcontractors' employees to comply with and uphold data protection and data security requirements	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	5. Process for informing and notifying the Controller before subcontracting and/or processing personal data	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE

7. Monitoring availability and capacity (availability monitoring)

It must be ensured that personal data are protected from accidental destruction or loss.

Implemented?	Measure	Comment
Yes	1. Documented concept for data backup and recovery	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE The operating manuals must cover the following areas: Data backup (e.g., type, scope, schedule, procedure, recovery, retention period, erasure plan) and job scheduling
Yes	2. Redundant storage systems	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Backup data must be stored in a location with different threat profiles than the location containing the production data.
Yes	3. Separate storage of data and backup data	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Backup data must be stored in a location with different threat profiles than the location containing the production data.
Yes	4. Protection from environmental damage (e.g., fire, water, overvoltage)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	5. Availability of an uninterruptible power supply and emergency power supply	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE

Implemented?	Measure	Comment
Yes	6. Availability of an appropriate security concept	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE All developed, configured or integrated systems and applications that fulfill a function at DPDHL must satisfy clearly defined technical and functional criteria. Security requirements for information systems Objectives: Guarantee that information security is an integral part of information systems throughout their lifecycle. This includes requirements for information systems that provide services over public networks. Analysis and specification of security requirements, measures: 1. Requirements pertaining to information security should be included in the requirements for new information systems or improvements to existing information systems. 2. All information security requirements and risks for IT services, IT systems and IT applications must be identified, justified and accepted in the requirements definition phase of a project (before development and/or implementation). The security of IT services, IT systems and IT applications must be verified at regular intervals. 3. The security concept must include at least the following (*information about expanding the generic risk assessment and risk management): a) Results of an initial risk identification (*) b) Results of the security classification (*): i) Classification of information and data ii) Classification of IT services, systems, components and applications c) Identified information security requirements (e.g., technical, regulatory and functional) (*) d) Results of the risk assessment and risk management i) Structural analysis (*) ii) Identification of relevant threats iii) Risk classification based on likelihood of occurrence and impact e) Results of risk management i) Defined information security measures (*) ii) Implementation status of the information security measures (*) iii) Specified residual risks 4. The security concept and the identified residual risks must be adopted by the risk owner(s). 5. In accordance with the residual risks and the classes defined in the risk assessment and risk management, the security concept must be reviewed at regular intervals and kept up to date during operational use of the IT system, IT service or during their development. The triggers for a review and adaptation of a safety concept include changes to: a) Regulatory requirements b) The threat and risk situation and the risk assessment c) The information security requirements (risk acceptance criteria). 6. The security concept must be subject to strict version and change control.

Implemented?	Measure	Comment
Yes	7. Binding process for and execution of updates	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE In order to ensure that the latest approved patches and application updates are installed for all approved software, a software update process should be implemented. All changes are tested and documented in full so that they can be reused for future software updates if necessary.
Yes	8. Monitoring of the availability, functionality, security and usability of the processed data	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE System acceptance testing measures: 1. Acceptance test programs and associated criteria should be defined for new information systems, upgrades and new versions. 2. Before an IT system is accepted, the requirements of the security concept must be implemented and the user manual must be provided. New IT systems, security requirements, system updates and software versions must undergo a formal test and release procedure before they are introduced to the production environment. Criteria that cover at least the following aspects must be defined for the acceptance: a) Requirements concerning scope of service and computer performance b) Error handling and recovery process c) Preparation and testing of standard operating procedures according to the defined specifications d) Measures for maintaining operational processes in consideration of these proposals e) Evidence that the installation of the new IT system will not adversely affect existing IT systems, especially at peak times such as month-end closings f) Evidence that the new IT system will not adversely affect the overall security of DPDHL information processing g) Training in the operation or use of the new IT system h) Compliance with the information security policy and regulations, and with the relevant regulatory requirements 3. Testing should be performed in a realistic test environment to ensure that the system does not cause vulnerabilities in the organization's operating environment and that the tests are reliable.
Yes	9. Control and review of backup copies of processed data	Data backup measures: 1. Based on the information security risk assessment, data from all IT platforms and technologies used in production must be backed up and the effectiveness of the backup recovery tested. 2. Backups may only be used for authorized purposes and access to the backups may only be granted to authorized personnel. 3. Backup data must be stored in a location with different threat profiles than the location containing the production data.

Implemented?	Measure	Comment
Yes	10. Deployment and availability of security systems for protection against, e.g., cyber attacks (e.g., DDoS), intrusions (e.g., hardware and/or software firewall), damage (antivirus protection), ransomware (e.g., malware locks) and similar	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE 1. If technically feasible, malware protection must be present with identical and consistent efficacy in all DPDHL systems that are commonly vulnerable to malware infections. This includes the following systems at a minimum: a) Windows OS-based systems (e.g., servers, laptops, desktop PCs); b) File and document storage systems, e.g., network area storage (NAS) or web-based applications for document management and collaboration; c) Messaging solutions, e.g., e-mail services or instant messengers; d) Removable storage devices, e.g., USB drives or other portable storage devices; e) Network traffic toward end-user devices and servers (here such protection can be provided by intrusion prevention systems [IPS]); f) User internet traffic (here such protection can be provided by a secure web gateway[SWG] aka internet proxy). 2. If multiple anti-malware protection layers are used in a line, they must be designed differently (come from different developers) to apply the defense-in-depth principle as effectively as possible (e.g., different anti-malware solutions for network, IT application, server, desktop, etc.). 3. The malware software used and its malware definitions must be managed and updated without delay. 4. Based on the results of an information security risk assessment, the anti-malware protection systems must be accompanied by technical measures for host and/or network protection (e.g., intrusion detection system[IDS], intrusion prevention system[IPS]). 5. Anti-malware logs from the last 90 days (active + archive) must be retained for reporting and investigation purposes. 6. The automatic execution of macros from untrusted sources by desktop applications (e.g., MS Office) must be deactivated. 7. All IT systems, including but not limited to end user devices, without suitable malware protection (e.g., outdated signature files) must be isolated in a dedicated network segment. 8. Indicators of compromise must be defined for IT systems and regular scans must be performed to analyze all indicators. 9. All incoming electronic messages (e.g., e-mails, chat messages) from the internet or other sources external to DPDHL must be scanned for malware before being made available to the intended recipient. 10. Based on the information security risk assessment and the technical feasibility study, other electronic messages must be scanned for malware before being made available to the intended recipient. 11. The effectiveness of the anti-malware measures must be measured and reported regularly (e.g., provision of anti-malware protection system maintenance for signatures, software updates and patches, in particular version and signature status).

Implemented?	Measure	Comment
Yes	11. Regular maintenance of IT systems (hardware and/or software)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Mechanisms for protecting against information loss should be regularly updated and continuously developed to ensure that their configurations (e.g., rules) are appropriate for the sensitive data that are to be protected
Yes	12. Design and implementation of an appropriate concept for non-interruptible functioning that corresponds to the state of the art (hardware and/or software)	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE The operating manuals must cover the following areas: a) Security configuations (e.g., system hardening basic configuration); b) Patch management; c) Data backup (e.g., type, scope, schedule, procedure, recovery, retention period, erasure plan) and job scheduling; d) Training on the use of information media (e.g., use of special letter paper, handling highly confidential information including procedures for safe disposal of information from failed orders); e) Fault management (e.g., emergency, contingency and recovery plans, as well as support and escalation contacts).

8. Check that data are being processed for their intended purpose

It must be ensured that data collected for different purposes can be processed separately.

Implemented?	Measure	Comment
Yes	1. Segregation of clients	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Information security requirements regarding technical architecture must be regulated in order to guarantee the required availabilities; it must be ensured that there is an effective separation of data processing and data storage of different customers and that there is also separate client-oriented data storage by the provider.
Yes	2. Separation of functions	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Information security requirements regarding technical architecture must be regulated in order to guarantee the required availabilities; it must be ensured that there is an effective separation of data processing and data storage of different customers and that there is also separate client-oriented data storage by the provider.
Yes	3. Database separation	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Information security requirements regarding technical architecture must be regulated in order to guarantee the required availabilities; it must be ensured that there is an effective separation of data processing and data storage of different customers and that there is also separate client-oriented data storage by the provider.

Implemented?	Measure	Comment
Yes	4. Concept for client use/restriction of use	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Protection of external identities, customer data, employee data, and data from business partners (extension of the ISO standard) Identities and customer data, employee data, and partner data are special types of information that require additional protection.
Yes	5. Procedures for saving, editing, deleting or transferring data for different purposes	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Protection of external identities, customer data, employee data, and data from business partners (extension of the ISO standard) Identities and customer data, employee data, and partner data are special types of information that require additional protection.

9. Process for regular review, assessment and evaluation of data protection measures (data protection management system)

Measures to ensure the effectiveness of the technical and organizational measures taken in the long term, including all measures to ensure a structured data protection organization, secured by an appropriate data protection management system. At a minimum, this requires organizational structures (e.g., roles and responsibilities), organizational workflow measures (e.g., processes and procedures) and documented policies including associated process definitions.

Implemented?	Measure	Comment
Yes	1. Data protection management system available and implemented	DPDHL PRIVACY PORTAL The privacy portal is based on the software “One Trust”. The privacy portal is used to conduct data protection audits of IT systems and data protection organization audits, and to maintain the register of processing activities.
Yes	2. Data protection officer(s) and IT security officer(s) appointed and integrated into the Processor’s structures	DHL GROUP CORPORATE DATA PROTECTION POLICY An independent data protection contact (data protection officer/data protection coordinator) must be appointed for each Group company. The data protection officer is responsible for implementing standards and works to ensure compliance with the relevant regulations.
Yes	3. Independence of the data protection officer in issuing instructions in the course of performing their duties is guaranteed	DHL GROUP CORPORATE DATA PROTECTION POLICY An independent data protection contact (data protection officer/data protection coordinator) must be appointed for each group company. The data protection officer is responsible for implementing standards and works to ensure compliance with the relevant regulations.
Yes	4. Regular monitoring, review and optimization of the technical and organizational measures used	DHL GROUP CORPORATE DATA PROTECTION POLICY Provision of a process for regular review, assessment and evaluation of the effectiveness of technical and organizational measures for ensuring the security of processing.

Implemented?	Measure	Comment
Yes	5. Immediate notification of the responsible party in the event of security breaches and/or data leaks	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE If information is identified as personal data or personal data of a special nature: The legitimacy of the exchange/transfer of such information or data must be agreed with the data protection officer. Any loss of data or unauthorized third-party knowledge must be reported immediately as an information security incident.
Yes	6. Evaluation of notices and reports on unusual events	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	7. Regular specialist training of the IT managers and the data protection officer	DHL GROUP CORPORATE DATA PROTECTION POLICY Employees of Group companies must be given appropriate training on data protection and on the application of the Group Privacy Policy. --- DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE All employees must be informed of the existence, binding nature and content of the Information Security Policy and any additional policy. Furthermore, employees must be sensitized to, adequately informed of and, if necessary, instructed in information security and data protection at DPDHL.
Yes	8. Employee training on data protection and information security	DHL GROUP CORPORATE DATA PROTECTION POLICY Employees of Group companies must be given appropriate training on data protection and on the application of the Group Privacy Policy.
Yes	9. Creation of an incident management and reporting process	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE
Yes	10. Documented process for detecting and reporting security incidents and/or data breaches	DHL GROUP CORPORATE DATA PROTECTION POLICY If an information security breach is discovered or suspected, every employee must understand that DPDHL expects that the responsible user helpdesk will be informed immediately or another interface will be used for the report.
Yes	11. Logging and investigation of security incidents and/or data breaches	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Management of information security incidents and improvements: 1. Any loss of data or unauthorized third-party knowledge must be reported as an information security incident and, if personal data are affected, must also be reported immediately as a data breach. 2. Prompt handling of vulnerabilities must be ensured by way of organizational measures or processes, including reporting. All security vulnerabilities (including those already remedied) must be reported to information security management. Evaluation of and decisions concerning information security events, actions: Information security events should be evaluated, and a decision should be made as to whether to classify them as an information security incident.

Implemented?	Measure	Comment
Yes	12. Defining, documenting and ensuring binding data protection and information security guidelines	DHL GROUP DATA PRIVACY POLICY 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. It is aimed at creating an adequate level of protection for the transfer of personal data from Group companies established in the European Union (EU) to Group companies in third countries without an appropriate level of data protection.
Yes	13. Performance of audits of subcontractors with respect to data privacy and information security requirements	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Usually by way of external audits or certifications, e.g., ISO Monitoring and review of supplier services, measures: Organizations should regularly monitor, review and audit the provision of services by suppliers. The services, reports, and records provided by third parties must be monitored and reviewed on a regular basis, and compliance assessments should be performed regularly.
Yes	14. Protection against the transfer and use of real data to/in test or development systems	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Protection of test data, measures: 1. Test data should be deliberately selected, protected and controlled. Functional and operational acceptance tests usually require large quantities of data that need to resemble operational data as closely as possible. 2. The use of operational data containing personal information and the use of real data in tests are generally not permitted. Where the use of real data cannot be avoided, the following measures should be taken to protect the data for testing purposes: a) All security controls that apply to operational data must be applied in the same manner for the data used in the test b) The access control procedures that apply to operational application systems must be used in the same manner for the application systems in the test c) If unavoidable, the copying and use of real data should be performed by additional special user accounts and a log must be kept so that an audit trail can be made available d) In the exceptional case that real data have to be used, they must be anonymized or pseudonymized beforehand e) It must be ensured that the anonymization or pseudonymization is adequate and no data leakage threats are present, e.g., if external IT service providers are involved f) Information from IT systems used in regular operations (so-called “real data”) must be erased from the test environment as soon as the test is complete

Implemented?	Measure	Comment
Yes	15. Control and amendment of data protection and information security specifications on the basis of applicable legal regulations	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Compliance with legal and contractual requirements Objectives: To avoid violations of legal, official or contractual obligations related to information security, as well as any security requirements. To determine applicable laws and contractual requirements; measures: 1. All relevant legal, regulatory and contractual requirements, as well as the organization's approach to meeting those requirements, should be explicitly defined, documented and continuously updated for each information system and for the organization. 2. Depending on the business purpose, the responsible division must systematically define legal obligations, guidelines and other requirements, as well as derive regulations, define measures and implement them, for example, as part of the security concept and during contract negotiations with IT service providers. Identifying applicable legislation is the fundamental prerequisite for IT compliance. Regular monitoring must be ensured by defining and implementing appropriate technical and organizational measures.
Yes	16. Compliance with the principles of "privacy by design" and "privacy by default"	DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE Personal data and information must be kept under control in accordance with local data protection laws and the Data Privacy Policy. The principles of data protection through "privacy by design" and "privacy by default" must be upheld.
Yes	17. Creating and updating a register of processing activities pursuant to Art. 30 GDPR	DHL GROUP CORPORATE DATA PROTECTION POLICY The Controller shall take appropriate measures to provide the data subject with information about the processing in a meaningful, transparent, understandable and easily accessible form. The information shall be provided in writing or via other means where appropriate.

III. ANNEX – LIST OF SUB-PROCESSORS

(Sub-)Processor

Company	Address	Service Description/ Duration of the Processing
Micromata GmbH	Marie-Calm-Straße 1-5, D-34131 Kassel	Operation of rapid mailbook system
Materna SE	Voßkuhle 37, D-44141 Dortmund	Maintenance and operation of GK portal system
T-Systems International GmbH	Hahnstraße 43d, D-60528 Frankfurt am Main	Operation of cloud infrastructure

Data Center/Centers of the Processor and/or Sub-Processor:

Company	Country	Address
Microsoft	Netherlands	Agriport 601 1775 TK Middenmeer Netherlands