

DHL Korea Ltd.

Personal Information Management Policy (V1.1)

DHL Korea Ltd. (www.dhl.co.kr, the “Company” or “DHL Korea”) abides by the provisions applied to information and communications service providers under the laws related to protection of personal information, including the Personal Information Protection Act (the “PIPA”), the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. (the “APIC”), and the Use and Protection of Credit Information Act.

For the purpose of the foregoing, DHL Korea implements and operates this Personal Information Management Policy (the “Management Policy”) pursuant to Article 30 of the PIPA and Article 27-2 of the APIC in order to protect personal information and the rights of the subjects of relevant personal information (the “Information Subject”) and smoothly handle and manage complaints raised by Information Subjects.

In case of amending this Management Policy, the Company shall notify any amendments on the Company’s website.

This Management Policy shall be amended as follows and take effect from December 15, 2018.

Article 1 Purpose of Handling Personal Information

The Company shall handle personal information for the purposes described below. The Company shall not use any personal information which the Company handles for purposes other than those described below. If the purpose of use is changed, the Company will take adequate measures including obtaining a separate consent pursuant to Article 18 of the PIPA and Article 24 of the APIC

1. Providing of Services

The Company handles personal information for purposes of verification of the identity of the customer, providing of contents, reservation for delivery, delivery of products, sending of contracts and invoices, providing of customized services, settlement and calculation of payables, responding to customers’ inquiries and requests related to delivery, providing of updates and materials.

2. Handling complaints

The Company handles personal information for purposes of verification of the identity of the customer who raises complaint and the details of the relevant complaint, communication and notice for the purpose of inspecting facts, notification of the result, etc.

3. Marketing and Promotional Activities

The Company handles personal information for purposes of general marketing

activities including providing of information related to the Company's services via telephone, SMS, e-mail or DM, conducting promotional events or other various events, etc.

4. Management of Visitors and Mails

The Company handles personal information for purposes of providing visitor's cards to prevent unauthorized entrance to the offices, management of visitors, prevention of security accidents and terrorist activities, and understanding circumstances in case of accidents.

Article 2 Personal Information to be Handled

The Company shall collect the minimum personal information necessary to provide various services as follows:

1. Title of the Personal Information File: general information related to inquiries on delivery services
 - Contents of personal information (mandatory): name, e-mail
 - Contents of personal information (optional): telephone number, company, department
 - Manner of collection: via company website, telephone / e-mail
2. Title of the Personal Information File: general information regarding delivery services
 - Contents of personal information (mandatory): name of the sender and recipient, country, company, email, address, telephone number
 - Contents of personal information (optional): title, department
 - Manner of collection: via the DHL shipping Solutions / telephone / e-mail / document etc.
3. Title of the Personal Information File: general information regarding Passport delivery service
 - Contents of personal information (mandatory): residential country, consulate, applicant name, passport owner (name, date of birth), telephone number, e-mail
(If Credit card selected as Payment method) Card company, Card number, Expiry date
 - Manner of collection: via company website
4. Title of the Personal Information File: general information regarding partnership companies
 - Contents of personal information (mandatory): name, company name, business registration number, bank account number, address
 - Contents of personal information (optional): name of the person in charge, telephone number, email, fax number
 - Manner of collection: via e-mail / document

5. Title of the Personal Information File: general information of job applicants
 - Contents of personal information (mandatory): name, address, telephone number, mobile phone number, e-mail, educational background, military service record, disability, other matters provided by the relevant applicant in his/her cover letter and resume
 - Contents of personal information (optional): information related to family members, certificates, work experiences, language skills, etc.
 - Manner of collection: via company website and e-mail

6. Title of the Personal Information File: general information regarding campaigns or event landing pages
 - Contents of personal information (mandatory): name, e-mail, address of the company, mobile phone number
 - Manner of collection: via webpages for the campaigns

7. Title of the Personal Information File: other automatically generated information
 - Contents of personal information (mandatory): access IP information, cookies, service use record, access log.
 - Manner of collection: via tool for collecting generated information

8. Title of the Personal Information File: import clearance
 - Contents of personal information (mandatory): nationals – recipient's name, personal customs code, address, telephone number, e-mail / foreigners - recipient's name, address, telephone number, e-mail
 - Manner of collection: via e-mail

9. Title of the Personal Information File: Voice of Customers
 - Contents of personal information (mandatory): name, mobile phone number, e-mail
 - Contents of personal information (optional): telephone number, address, company name, waybill number, account number
 - Manner of collection: via company website

10. Title of the Personal Information File: Visited outbound shipment customer
 - Contents of personal information (mandatory): name, e-mail, phone number, address
 - Manner of collection: via document

Article 3 Handling and Retention Period of Personal Information

- ① The Company shall retain and use personal information related to providing of services for the period provided under the applicable laws or specified in the letter of consent of the relevant Information Subject at the time of collecting the relevant personal information, or from the date of the letter of consent for use and collection to

the date on which the purpose of handling the personal information is satisfied; provided, that the Company may retain and use the personal information after the expiration of the applicable retention period for the sole purpose of handling complaints and performing obligations under the applicable laws.

② In principle, each personal information shall be handled and retained until completion of the delivery of the services and of settlement and calculation of payables; provided, that in the following cases, the Company shall handle and retain the relevant personal information until the relevant cause for retention is terminated:

1. In cases where investigation or inspection is ongoing for a violation of applicable law, until the completion of the investigation or inspection
2. Records on transactions such as labeling advertising, terms and performance of a contract, in accordance with Article 6 of the Enforcement Decree of the Act on Consumer Protection in Electronic Commerce, etc.
 - Records on labeling advertising: six (6) months
 - Records on revocation of a contract or an offer, payment of price or providing of goods: five(5) years
 - Records on customer complaints or dispute resolutions: three (3) years (provided, that, records on claims shall be retained for five (5) years)
3. Records on telecommunications, in accordance with Article 41 of the Enforcement Decree of the Protection of Telecommunications Secrets Act
 - Records on date of telecommunications, opening time and closing time, registration number of the counterparty, points used, tracking records on the location of the base station used in the telecommunication: one (1) year
 - Records on computer communication, internet log, tracking records on the location of access: three (3) months
4. Records on identification, in accordance with Article 29 of the Enforcement Decree of the APIC, for six (6) months after removal of posting on the bulletin board
5. Evidential records of transactions, in accordance with Article 85-3(2) of the Framework Act on National Taxes, Article 116(1) of the Corporate Tax Act, Article 31 of the Value-added Tax Act, etc., for five (5) years after the report deadline.
6. Request letter for change of payment terms and confirmation letters from recipients, one (1) year and six (6) months after submission to the Ministry of Strategy and Finance.
7. Records of management of visitors (their entrance) and mails, for one (1) year.

Article 4 Providing Personal Information to Third Parties

- ① In principle, the Company shall handle the personal information of Information Subjects within the scope of purposes set forth in Article 1 of this Management Policy. The Company shall not handle or provide to third parties any personal information beyond the originally intended scope if not for cases provided under Articles 17 and 18 of the PIPA and Articles 22 and 24-2 of the APIC (prior consent from the relevant Information Subject, exceptional legal provision, etc.)
- ② The Company provides personal information to third parties as follows

Transferee	Purpose of Use of Personal Information by Transferee	Contents of Personal Information Transferred	Period for Maintaining and Use of Transferee
Korea Customs Service (125)	Imposing/collecting duties and tax, Declaration of shipment	Name, E-mail address, contact number (office, home, mobile, fax), address (home, office)	Until fulfillment of the purpose
National Tax Service (126)	Imposition, exemption, and collection of various taxes, including V.A.T.	Name, E-mail address, contact number (office, home, mobile, fax), address (home, office)	Until fulfillment of the purpose

Article 5 Outsourcing of Handling of Personal Information

- ① The company shall outsource the handling of personal information for the purpose of effective management of the affairs related to the personal information as follows.

Outsourcing Company	Outsourced services
Deutsche Post AG (Germany)	Overseas shipping
Affiliates of Deutsche Post DHL Group (subprocessors) For full list of affiliates, please refer to full list	Overseas shipping
Korean Air Asiana Air Polar Airline China Southern Airlines (Raon Air) Shandong Airlines (Borim T&L) Dalavia-Far East AF-KL Cargo Air Incheon Airbridgecargo Emirates Airline	Overseas shipping

Aeroflot Airlines Miat Mongolian (iforward) Etihad Cargo China Airlines	
Deutsche Post DHL Group IT Center Overseas, DHL IT Services	Data processing and storage
UnSeo Customs Co. Ltd.	Customs brokerage service
DHL Asia Pacific Finance Shared Services Center	Registration and management and retention of partner companies
I2S	Printing and shipping
Humming IMC Purple INC	Events, shipping prize
KyoungDong R&D AnyQuick Volt Technology Hana fine logistics Hayoung DongBang Transport Logistics Co Ltd Jeju Air Ocean DaDa Global Baeg Ma Logistics Ilyang Logisticts CVS Net (GS25) Aeris Korea Korail Networks Mirae Ducksoo	Domestic transportation
Biztalk iHeart	Mobile messages (SMS) transmission
Midas IT	Development and maintenance for the HR recruit site
NICE AMC	Debt collection service
Global Collect B.V. (Ingenico) KGInicis	Credit card payment processing
Eber	Membership point management

- ② Upon entering into an outsourcing agreement, the Company shall specifically set forth the matters, including without limitation prohibition of handling of personal information for purposes other than performing the outsourced services, technical and managerial protection measures, management and supervision of the outsourcing company, matters related to the compensation for damages and suboutsourcing in the agreement or other relevant documents in accordance with Article 26 of the PIPA and Article 25 of the APIC in connection to such outsourcing, and supervise the outsourcing company to safely handle personal information.
- ③ In case of change in the outsourced affairs or outsourcing companies, the Company shall immediately notify such change via this Management Policy.

Article 6 Rights and Obligations of Information Subjects and their Legal Agents, and Performance thereof

- ① An Information Subject and a legal agent may exercise the following rights related to protection of personal information on behalf of himself/herself or the concerned child under age of 14:
 1. Request to access personal information;
 2. Request to correct personal information (in case of errors, etc.)
 3. Request to remove personal information; and
 4. Request for suspension of handling personal information.
- ② The rights set forth in Paragraph 1 may be exercised by in writing, via telephone, e-mail, fax, etc., and the Company shall immediately take necessary measures after verifying the identity of the relevant Information Subject.
- ③ If an Information Subject or a legal agent requires for removal or correction of any errors in personal information related to himself/herself or the concerned child under age of 14, then the Company shall not use or provide the relevant personal information until the correction or deletion is completed. The Company shall immediately rectify any wrongful use or providing of personal information upon detecting the same.
- ④ Rights set forth in Paragraph 1 may be exercised through a legal agent (legal representative, proxy, etc.). In such case, a power of attorney in the form as prescribed in APPENDIX 11 of the Enforcement Rules to the PIPA shall be submitted to the Company.
- ⑤ No Information Subject shall infringe any personal information and privacy of him/herself or a third party which the Company is handling, in violation of the applicable laws including the PIPA or the APIC.

Article 7 Destruction of Personal Information

- ⑥ Unless there is a justifiable cause under Article 6 of the Enforcement Decree of the Act on Consumer Protection in Electronic Commerce, etc., Article 41 of the Enforcement

Decree of the Protection of Communications Secrets Act, Article 29 of the Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., or any other law to retain personal information, the Company shall destroy the concerned personal information within 5 days after the expiration of the applicable retention period.

- ⑦ In case where the Company shall, pursuant to any other law, retain personal information after the expiration of the applicable retention period or satisfaction of the purpose of handling the relevant personal information, the Company shall transfer the relevant personal information into a separate DB or store the same in a separate storage location.
- ⑧ The Company shall select personal information which shall be destroyed, and destroy the selected personal information upon approval of the Personal Information Protection Manager.
- ⑨ Electronic files containing personal information shall be destroyed in a technical manner that does not allow restoration of the personal information, and print-outs containing personal information shall be shredded or burnt.

Article 8 Procurement Measures for the Safety of Personal Information

The Company shall take technical, managerial and physical measures necessary in accordance with Article 29 of the PIPA and Article 28 of the APIC as follows:

1. Managerial Measures: Implementation and operation of the Personal Information Internal Management Plan, minimization and training of employees who handle personal information
2. Technical Measures: Security measures using technology including encryption, installation of security devices, measures to prevent fabrication/falsification of access record, measures to prevent computer viruses such as installation and operation of vaccine programs
3. Physical Measures: Restriction and control of access to computer room, documentation storage room, etc.

Article 9 Installation, Operation and Refusal of Devices that Automatically Collect Personal Information

- ① The Company shall use 'cookies' which saves and loads user information in order to provide optimized information to the website users by collecting and analyzing types of visits and uses of the websites, and the number of users.
- ② The website users may choose whether or not to install the cookie. Therefore, the users may allow every cookie to be saved, confirm each time when a cookie is saved, or refuse to save any cookie by changing the option on the web browser.

Article 10 Personal Information Protection Manager

The Company appoints a personal information management/protection manager and working-level officer in order to protect personal information and handle any complaints related to the personal information in accordance with Article 31(1) of the PIPA and Article 27 of the APIC as follows:

1. Personal information protection officer
 - Department: IT
 - Contact information: selhelpdesk@dhl.com
2. Personal Information Protection Department
 - Department: Security team
 - Contact information: krsid@dhl.com

Article 11 Installation and Operation of Visual Data Processing Equipment

The Company shall install and operate visual data processing equipment as follows:

1. Reasons for and purpose of installation visual data processing equipment:
Securing the safety of the Company's facilities and preventing fire, etc.
2. Place of installations and locations filmed : installed inside and outside of the major facilities of the Company such as lobby, entrances and emergency exits; entire spaces of the major facilities are filmed
3. Management officer, department in charge and the person who has right to access visual data: Manager of Security team
4. Time of filming, retention period, storage place and methods of handling visual data
 - Time of filming: 24 hours
 - Retention period: 30 days (no more than 30 days in cases of CCTVs installed on sales services points, no more than 24 hours if installed in customer centers)
 - Storage place and handling methods: Maintenance manager of each facility or a delegated person shall separately retain and handle the relevant visual data.
5. How and where to review visual data: by request to the maintenance manager of each facility
(If a customer or other person who is not an officer or an employee of the Company requests for visual data, the relevant visual data shall be provided and confirmed upon the final approval of Personal Information Management/Protection Manager.)

6. Measures to be taken in relation to request made by Information Subject to access visual data: The request shall be made via a “request to access·confirm existence of personal information,” and access is allowed only when the concerned Information Subject is filmed or if evidently necessary for interests of life, body and properties of the concerned Information Subject.
7. Technical, managerial and physical measures to protect the visual data: establishment of the Personal Information Internal Management Plan, restriction and control of access to visual data, implementation of technologies related to saving and transferring visual data, retention of handling record and measures to prevent falsification and fabrication of the same, and acquiring of storage facilities and installation of locking devices.

Article 12 Remedies against Infringement of Rights

The Information Subjects may apply for consultations to the Personal Information Dispute Resolution Committee, Personal Information Infringement Reporting Center of the Korea Internet Security Agency, etc. in order to remedy infringement of personal information. With regard to other reports on infringement of personal information and counseling, please contact the following organizations:

1. Personal Information Dispute Resolution Committee: (without area code) 118;
2. Personal Information Protection Mark Certification Committee: +82-2-580-0533~4
3. Supreme Prosecutors’ Office, Cybercrime Investigation Division: +82-2-3480-3573
4. National Policy Agency, Cyber Terror Response Center: +82-2-1566-0112

Article 13 Amendment of Personal Information Management Policy

This Management Policy shall come into effect from the implementation date. In case of any insertion, deletion or correction is made in accordance with the applicable laws and guidelines to the provisions of this Management Policy, the Company shall make notice of such modification no later than 7 days prior to the implementation date of the modified provisions.