Deutsche Post DHL Group

DEUTSCHE POST DHL GROUP

INFORMATION SECURITY CODE OF PRACTICE FOR PARTNERS

Document Owner: DPDHL Group CISO

Version: 3.0

Date issued: January 2022

Table of Contents

Part 1: DPDHL Group: Introduction to Security Requirements

1) DPDHL Group uses, creates and stores a significant amount of data in the course of its business and must ensure that the confidentiality, integrity and availability of data is protected. DPDHL Group expects and requires all suppliers to DPDHL Group to implement and maintain appropriate and effective safeguards and controls to ensure the security of DPDHL Systems and information.

2) Capitalised terms used in the ISCOP shall have the meaning assigned to those terms in the definitions section at Part 4 of the ISCOP, unless the context requires otherwise. Where the ISCOP forms part of any agreement between the Supplier and a member of DPDHL Group, the definitions provided within the ISCOP shall prevail over any conflicting definitions in the remaining part of such agreement, but only with regards to the interpretation of the ISCOP.

3) Part 2 of the ISCOP sets out mandatory minimum security requirements with which DPDHL Group expects the Supplier to comply. If the Supplier is unable to comply with these minimum security requirements, it will not be able to enter into any agreement with DPDHL Group.

4) Part 3 of the ISCOP sets out enhanced controls with which all suppliers should seek to comply. Further, if the Supplier meets any of the following criteria then it must comply with the enhanced controls in Part 3 of the ISCOP:
   a) the Supplier Processes DPDHL Data using Supplier systems outside DPDHL Group premises; and /or
   b) the Supplier has access to DPDHL Systems, whether via remote access or otherwise.

5) Where the Supplier Processes Personal Data on behalf of DPDHL Group and/or the Supplier Processes Personal Data outside of the European Economic Area, additional requirements and expectations pursuant to Data Protection Legislation will be included in the relevant agreement between the Supplier and the relevant member of DPDHL Group. To the extent that those additional measures overlap or conflict with requirements set out in the ISCOP, the more stringent requirements of the two shall apply to the Supplier.

Part 2: Mandatory Minimum Security Requirements

1) In addition to the below mandatory minimum security requirements, the Supplier should manage information security in accordance with the practices described in ISO 27001.

2) Where any part of the Services are not covered by the scope of a current ISO 27001 certification, the Supplier should at all times and upon request be able to demonstrate it has implemented controls equivalent to industry standard controls such as ISO/IEC 27002:2013.

3) DPDHL Group may, at its own discretion, conduct information security audits relating to the supply of Services by the Supplier. Details regarding DPDHL Group's right to audit are set out below.

4) The Supplier shall comply with the following mandatory minimum security requirements:

Table A – Minimum Security Requirements

Requirement	Expectation
General	
Preservation of confidentiality, integrity and availability	The Supplier shall be responsible for preserving the integrity of DPDHL Data and preventing the corruption or loss of DPDHL Data and shall ensure that it has in place appropriate controls (including with its agents, contractors or sub-contractors) to guard against unauthorised and/or unlawful use of DPDHL Data.
System security	The Supplier shall ensure that any system on which the Supplier holds any DPDHL Data, including back-up data, is a secure system that complies with Part 3 of the ISCOP, and in particular only enables access to DPDHL Data in electronic form to Supplier Personnel to the extent necessary to provide the Services.
Requirement	**Expectation**
Information and Cyber Security Protection	
Protecting Information	The Supplier must protect DPDHL Data throughout its lifecycle and shall maintain an inventory of DPDHL Data in the Supplier's possession (and also in the possession of any sub-contractor). The Supplier must provide DPDHL Group with evidence to demonstrate that controls are in place to protect and manage DPDHL Data in accordance with its classification.
Information Security Testing	Where the Supplier hosts a web site or externally facing application which stores, Processes or transmits DPDHL Data or displays DPDHL Group branding, or where a DPDHL Group internal address space is extended to the Supplier's network, the following requirements shall apply. To the extent that the Supplier has agreed to comply with DPDHL Group requirements which overlap or conflict with the requirements set out below, the more stringent requirements of the two shall apply to the Supplier: 1) that security testing, including penetration testing, is performed by a skilled independent service provider who is accredited by an industry recognized security testing body prior to the pages being hosted on the Internet; 2) there is a regular security testing schedule of the web site, occurring at a frequency of at least annually. The times and dates of the security testing are to be agreed by mutual consent of both parties; 3) DPDHL Group is provided with a summary of the results of the penetration testing, together with a list of remedial actions for each finding, where each action has a delivery date; and 4) progress on remedial action is reported monthly to DPDHL Group.
Requirement	**Expectation**
Information Security Incident Management	
Response Plan	The Supplier shall maintain a written Information Security Incident response plan and provide a copy of the plan to DPDHL Group upon request. The Supplier shall remedy each Information Security Incident in a timely manner following its Information Security Incident response plan in accordance with Good Industry Practice.

Requirement	Expectation
Notification Requirements	The Supplier shall notify DPDHL Group of any Information Security Incident affecting any DPDHL Data or DPDHL Systems managed or interfaced by the Supplier within 48 hours of becoming aware of the Information Security Incident. The Supplier shall use reasonable endeavours to provide a full report of the Information Security Incident and the related response as well as ensuring they reconstruct any lost or destroyed information without any charge to DPDHL Group. In case of an Information Security Incident or a Personal Data breach (as defined by Data Protection Legislation) affecting DPDHL Data, the Supplier shall report this to supplier-cybersecurity@dpdhl.com and to its defined DPDHL Group business contact.
Cooperation with DPDHL Group's Investigations	The Supplier shall reasonably cooperate with DPDHL Group in handling an Information Security Incident, including, but not limited to, the following: 1) coordinating with DPDHL Group on the Supplier's response plan; 2) assisting with DPDHL Group's investigation of the Information Security Incident; 3) facilitating interviews with the Supplier Personnel and others involved in the Information Security Incident or response; and 4) making available all relevant records, logs, files, data reporting, forensic reports, investigation reports, and other materials required for DPDHL Group to comply with applicable laws, regulations, or industry standards, or as otherwise required by DPDHL Group.
Third party notifications	The Supplier agrees that it shall not notify any third party (including any regulatory authority or customer) of any Information Security Incident on behalf of DPDHL Group without first obtaining DPDHL Group's prior written consent, unless this violates any existing law or regulation. Further, the Supplier agrees that DPDHL Group shall have the sole right to determine 1) whether notice of the Information Security Incident is to be provided to any individuals, regulators, law enforcement agencies, or others; and 2) the form and contents of such notice.
Requirement	**Expectation**
Data Protection Legislation Requirements for the Supplier	
Legal compliance	1) The Supplier shall adhere to applicable Data Protection Legislation, including provisions concerning the security of Personal Data, and to relevant regulations, such as GDPR; 2) The Supplier shall comply with all said requirements when Personal Data, in particular that of customers, consumers, employees and shareholders, is collected, recorded, hosted, Processed, transmitted, used, and / or erased; and 3) The Supplier shall comply with any contractual requirements on data protection and information security and shall not disclose any information that is not known to the general public.

5) Where the Supplier requires access to DPDHL Group internal information and systems the following apply:

Table B – Conditions of Supplier Access to DPDHL Group Internal Information and DPDHL Systems

Requirement	Expectation
Access on a need to know basis	The Supplier's access to any DPDHL Data shall only be granted to the Supplier when a need to know exists and when such a disclosure has been expressly authorized by a representative of DPDHL Group.
Legitimate and documented business need	Inbound access to DPDHL Systems shall only be granted to the Supplier where the relevant DPDHL System manager determines that the Supplier has a legitimate and documented business need for such access, and the systems of the Supplier provide no significant threat to any part of DPDHL Group infrastructure. The Supplier access shall only be enabled for specific individuals and only for the time period required to accomplish approved tasks.
Follow DPDHL Group network access onboarding procedures	The Supplier shall follow DPDHL System access onboarding procedures to obtain inbound access to DPDHL Systems. Such procedures include required information provision as part of network configurations including, but not limited, to IP addresses, network protocol, and network access implementation method (e.g. VPN setup).
Documentary evidence of an Information Security Management System	Before an account ID can be issued to the Supplier, documentary evidence of an information security management system or process shall be provided to and approved by DPDHL Group management and the Supplier shall agree in writing to prevent unauthorized and improper use of DPDHL Systems made available to the Supplier.
Immediate termination	DPDHL Group also reserves the right to immediately terminate network connections with all Supplier systems if DPDHL Group believes either that the Supplier is not meeting these requirements, or if the Supplier is providing an opportunity for attack against DPDHL Systems.
Documented security architecture	The Supplier shall maintain documented security architecture of the networks managed by the Supplier in its operation of the Services provided to DPDHL Group. The Supplier shall review the network architecture, including measures designed to prevent unauthorized network connections to all systems, applications, and network devices on a regular basis (i.e. at least once a year).
Separation of DPDHL Systems and Supplier systems and infrastructure	DPDHL Systems shall be strictly separated from the Supplier's internal systems and infrastructure.
Data logging	The Supplier shall collect all logging data relating to DPDHL Group (proof, evidence of actions) and shall provide this data to DPDHL Group without having been asked to do so or to grant DPDHL Group continuous access to it.

6) DPDHL Group shall have the following audit rights over the Supplier. To the extent that the Supplier has agreed to audit rights for DPDHL Group which overlap or conflict with the rights set out below, the more extensive audit rights for DPDHL Group of the two shall be exercisable by DPDHL Group:

Table C – Right to Audit for DPDHL Group

Requirement	Expectation
Audit Access	The Services and IT systems provided by the Supplier shall be subject to audit by DPDHL Group (or any external auditors as DPDHL Group may appoint) within reasonable written notice (including, but not limited to, data processing agreements concluded by the Supplier being compliant with Data Protection Legislation).
Audit Findings	The Supplier shall mitigate all findings identified in the audit within a commonly agreed timeframe and provide evidence of successful mitigation to DPDHL Group.
Evidence of Compliance	Upon request by DPDHL Group (not more often than once every twelve months), the Supplier shall provide evidence of compliance for the provisioned Services and IT systems in the form of independent review from third party auditors or industry recognized security assurance standards. The evidence provided shall comprise: 1) A copy of its annual certification of compliance with ISO 27001 and/or SSAE SOC2 or any equivalent reports; and 2) A copy of its vulnerability assessment and / or penetration testing reports relating to systems and processes involved in the provision of the Services (including product and version of application that has been concluded as compliant). Confidential and / or sensitive information may be removed in the report to protect the confidentiality of the Supplier's systems. However, the total number and severity of the identified issues shall be provided including risk mitigation measures and implementation timeline.
Requests for Information	Upon request by DPDHL Group, the Supplier shall provide answers and evidence to DPDHL Group contained in a 'Request for Information' (RfI) regarding the Supplier's information security and data protection risk and compliance.

Part 3: Enhanced Security Requirements

1) These enhanced security requirements set out in summary the technical and organisational information security control requirements that the Supplier must adopt when:
   a) the Supplier is Processing DPDHL Data using Supplier systems outside DPDHL Group premises; or
   b) the Supplier has access to DPDHL Systems, via remote access or otherwise.

2) These enhanced security requirements shall apply in addition to any requirements relating to information security practices and data protection standards set out in any agreement between the Supplier and DPDHL Group.

Table D – Enhanced Security Requirements

ISO Chapter/Control	Requirements
Organisation of Information Security	The Supplier must have a coordinated approach to information security. In particular, the Supplier's information security management system must consist of the following: 1) A set of regularly reviewed information security policies that must be defined and implemented; 2) All information security responsibilities must be defined and allocated; 3) Conflicting duties and areas of responsibilities must be segregated to reduce opportunities for unauthorised and unintentional modification or misuse of DPDHL Group's assets; 4) Appropriate contacts with relevant authorities, special interest groups or other specialist security forums and professional associations, which must be maintained; 5) Information security measures must be addressed in project management, regardless of the type of project; 6) Defined security measures / controls to manage the risks introduced by using mobile devices and remote working; and 7) The policies for information security must be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
Human Resource Security	The Supplier must have established measures to mitigate people security risks prior to employment, during employment, and after termination of employment. In particular, the Supplier must: 1) Carry out background checks and screening on all Supplier Personnel candidates; 2) Incorporate Supplier Personnel information security responsibilities into contractual agreements, policies and procedures; 3) Deliver information security awareness education and training at a regular and defined interval; and 4) Have formal disciplinary measures for Supplier Personnel who breach information security policies.
Asset Management	The Supplier must implement measures to manage information security assets throughout their lifecycle. In particular, the Supplier must: 1) Identify assets associated with information and information processing facilities and draw up and maintain an inventory of these assets; 2) Ensure assets maintained in the inventory have a named business owner; 3) Ensure rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented;

ISO Chapter/Control	Requirements
	4) Ensure all Supplier Personnel and external party users return all of the DPDHL Group and/or Supplier assets (as applicable) in their possession upon termination of their employment, contract or agreement; and 5) Classify, label and handle information assets in terms of legal requirements, value, criticality and sensitivity.
Access control	The Supplier must implement access control measures to protect information assets and resources. In particular, the Supplier must: 1) Establish and implement policies and procedures for access control (including onboarding, off-boarding and cross boarding users) and privileged access management; 2) Provide access based on principle of least privilege and segregation of duties; 3) Define and communicate user responsibilities in the use of secret authentication information; 4) Review user access rights at regular intervals; 5) Restrict the use of utility programmes that may be capable of overriding system and application controls; and 6) Implement password policies and usage of multifactor authentication technologies in line with risk and best practice.
Cryptography	The Supplier must implement cryptographic controls in alignment with industry-accepted standards. In particular, the Supplier must: 1) Define and implement a policy to define mandatory encryption measures in alignment with information classifications; and 2) Define and implement a policy on the use, protection, and lifetime of cryptographic keys.
Physical and Environmental Security	The Supplier must have measures to maintain security within physical sites and premises (e.g. offices, warehouses, data centres). In particular, the Supplier must define and implement security controls to protect: 1) Physical security perimeter and points of entry; 2) Offices, rooms, facilities, secure areas and delivery and loading areas; 3) Equipment (e.g. operational technology), supporting utilities, power and telecommunication cabling; 4) Procedures for working in secure areas, which shall be designed and applied; and 5) Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises. Access points shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
Operations Security	The Supplier must implement controls to protect information assets and information processing facilities. In particular, the Supplier must: 1) Define and implement policies and procedures for change management, capacity management, and operations; 2) Segregate development, testing, and operational environments;

ISO Chapter/Control	Requirements
	3) Implement controls to detect, prevent and respond to malware; 4) Create and maintain backups of information, software and system images at regular and defined intervals; 5) Maintain event logs of user activities and system administrator / operator activities, and secure logs against unauthorised access; 6) Synchronise all information processing system clocks to a single reference time source; 7) Control installation of software on operational systems; 8) Identify and remediate technical vulnerabilities in a timely manner; and 9) Carefully plan audit requirements and activities involving verification of operational systems and agree to minimise disruptions to business processes.
Communications Security	The Supplier must implement controls to maintain the security of information that is Processed and transferred through networks. In particular, the Supplier must ensure the following: 1) Networks should be managed and controlled to protect information in systems and applications. Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced. Groups of information services, users and information systems should be segregated on networks. Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities; 2) Agreements should address the secure transfer of business information between the Supplier and external parties; 3) Information involved in electronic messaging should be appropriately protected; and 4) Requirements for confidentiality agreements reflecting the Supplier's needs for the protection of information should be identified, regularly reviewed and documented.
System Acquisition, Development and Maintenance	The Supplier must integrate information security controls into all information systems and throughout the software development lifecycle. In particular, the Supplier must ensure the following: 1) Rules for the development of software and systems should be established and applied to developments within the Supplier; 2) When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on Supplier and/or DPDHL Group (as applicable) operations or security; 3) Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled; and ~~4)~~ The Supplier should supervise and monitor the activity of outsourced system development.

ISO Chapter/Control	Requirements
Supplier Relationships	The Supplier must manage risks associated with contracting third-party suppliers (i.e. fourth parties to DPDHL Group) that may access, Process, or store the Supplier's information assets. In particular, the Supplier must: 1) Have a third-party risk management policy that defines information security requirements to mitigate third party risks; 2) Establish and formally agree (i.e. within legally binding contracts) information security requirements with each third-party supplier; 3) Regularly monitor, review and audit each third-party supplier's service delivery; and 4) Manage changes to provision of services by third-party suppliers through maintenance of information security policies, procedures and controls.
Information Security Incident Management	The Supplier must have an established and documented process for identifying, assessing and responding to Information Security Incidents. In particular, the Supplier must: 1) Define roles and responsibilities pertaining to Information Security Incident management, including identifying key dependencies and escalation points; 2) Establish and communicate channels for reporting information security events (whether or not they are Information Security Incidents) or identified vulnerabilities / weaknesses; 3) Implement a methodology for triaging and classifying Information Security Incidents; 4) Conduct post-incident analysis exercises to continuously improve the Information Security Incident management process; and 5) Document and preserve evidence pertaining to an Information Security Incident.
Information Security Aspects of Business Continuity Management	The Supplier must embed information security continuity and resilience measures within its business continuity management systems. In particular, the Supplier must: 1) Develop policies, processes and plans to ensure information security continuity and continuity of information security management in adverse situations; 2) Conduct and document the results of testing of business continuity plans at regular and pre-defined intervals to ensure information security continuity controls are functioning as required; and 3) Implement redundancy measures to maintain availability of information processing facilities.
Compliance	The Supplier must ensure compliance with legal and contractual obligations and ensure internal compliance with information security policies and procedures. In particular, the Supplier must: 1) Define a governance cadence (i.e. required frequency of review) over the organisation's approach to managing and implementing information security Good Industry Practice; and

ISO Chapter/Control	Requirements
	2) Conduct reviews at regular and pre-defined intervals to assess compliance with information security policies, processes and standards.

Part 4: Definitions

1) The definitions in this Part 4 apply to the ISCOP.

"Affiliate"	(i) in relation to DPDHL Group, a legal entity which, presently or in the future, directly or indirectly, is Controlled by Deutsche Post AG or under common Control with Deutsche Post AG; and (ii) in relation to the Supplier, a legal entity which, presently or in the future, directly or indirectly, is Controlled by the Supplier or under common Control with the Supplier;
"Control" or "Controlled"	the controlling entity possessing, directly or indirectly, or jointly with a third party or parties, the power to direct management and policies of the controlled entity;
"Data Protection Legislation"	GDPR; the UK Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and, to the extent applicable, all other applicable laws and regulations of any other country relating to the Processing of Personal Data and privacy;
"DPDHL Data"	all data or records of whatever nature and in whatever form relating to the business, employees, customers, suppliers or otherwise relating to the business of DPDHL Group;
"DPDHL Group"	Deutsche Post AG and any Affiliate of Deutsche Post AG from time to time and a reference to DPDHL Group in the ISCOP shall be construed as a reference to all and any of them. It includes the relevant member of the DPDHL Group that is a party to any agreement with the Supplier to which the ISCOP forms part of such agreement;
"DPDHL Systems"	the information technology and communication systems, including networks, hardware, software, middleware, virtual platforms and interfaces owned by or licensed to DPDHL Group or any of its or their agents, customers or contractors;
"GDPR"	Regulation (EU) 2016/679 (the General Data Protection Regulation), including any amendments and updates in force from time to time;
"Good Industry Practice"	in respect of any activity, performing that activity effectively, reliably and professionally using the degree of skill, care, diligence, prudence, foresight and judgement which would reasonably be expected from a skilled and experienced operator of similar standing engaged in the provision of similar services;
"Information Security Incident"	1) any actual or suspected compromise of the confidentiality, integrity or availability of DPDHL Data; 2) any actual or suspected compromise of, or unauthorized access to, any system that Processes DPDHL Data that presents a risk to the confidentiality, integrity or availability of DPDHL Data; or 3) receipt of a complaint, report, or other information regarding the potential compromise or exposure of DPDHL Data Processed by Supplier;
"Internet"	the global network providing a variety of information and communication facilities,

	consisting of interconnected networks using standardized communication protocols;
"ISCOP"	DPDHL Group's Information Security Code of Practice for Partners;
"Process" or "**Processing"** or **"Processes"**	any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"Personal Data"	any personal data (as such term is defined in Data Protection Legislation) which is subject to the Data Protection Legislation;
"Services"	any or all of the services provided by the Supplier;
"Supplier"	the counterparty to any agreement with DPDHL Group to which the ISCOP forms part of such agreement; and
"Supplier Personnel"	the employees, contractors and other individuals who are engaged by the Supplier, its Affiliates or their subcontractors from time to time to meet the Supplier's obligations.