Data Protection and GDPR

dpdgroup

At DPDgroup UK Ltd (DPD & DPD Local) we take data protection seriously and have updated all our relevant policies and documents to ensure we meet the requirements of GDPR. We have compiled a comprehensive set of FAQs for our customers to cover every aspect of GDPR.

DPDgroup FAQs

Q1	Does DPDgroup consider itself to be a data controller and, if so, what are the implications?
	For our mobile App, 'Your DPD', we are the controller. For our customer data we are the processor.
Q2	How does DPDgroup ensure that suppliers it passes data on to are compliant with GDPR?
	All DPDgroup delivery sub-contractors/delivery partners are subject to GDPR due diligence to ensure that they meet the regulation standards required. All third party service suppliers adhere to our Supplier Data Obligations Policy (SDOP), which sets out the requirements for data protection and retention.
Q3	If a sub-processor is used, please confirm that a written agreement is in place with you and the sub-processor which imposes appropriate and GDPR compliant terms on the sub-processor.
	The DPDgroup contract entered into between the processor (DPDgroup) and its sub-processor (delivery partner) contain, the provisions stipulated in Article 28(3) of the GDPR, namely: • the subject matter and duration of the processing of personal data; • the nature and purpose of the processing; • the obligations of security, warning and alert towards the controller.
Q4	Are all employees and contingent staff required to agree and sign terms and agreements of confidentiality or non-disclosure and their responsibilities for information security?
	All employees are subject to the comprehensive DPDgroup IT User Charter, where employees are required to acknowledge and adhere to terms including (but not limited to) the following: A. General measures about remaining within the law B. Compliance with regulatory measures, e.g. copyright law, protecting relevant data C. Equipment protection and protection mechanisms (antivirus, patching etc) D. Data protection, i.e. data classification, confidentiality and leakage E. Specific measures relating to systems access, use of email and internet F. Monitoring measures used to ensure proper use of IT services G. Outcome of non-compliance, e.g. disciplinary procedure and/or civil or criminal law Additionally, our employees with system administration access to our IT systems sign up and adhere to our DPDgroup IT System Administrator Charter. We have relationships with external vendors to deploy advanced technology to provide us with an early warning against threats and build enterprise-wide prevention, protection, response and recovery capabilities. To demonstrate our ongoing commitment to information security we hold Cyber Essentials Plus certification which is backed by the UK National Cyber Security Centre. The date of the last internal parent group (La Poste) audit was March 2018.

Q5	Do all employees and contingent staff receive awareness training and regular updates as it relates to information security and other organisational policies and procedures relevant to their job function?
	All staff have received GDPR training as part of the overall comprehensive DPDgroup staff training programme. The comprehensive training programme is also delivered to all new starters and refresher training is given at regular intervals. Regular data privacy and security communication is provided to staff as well as phishing simulations and training.
Q6	Is access to personal data restricted to members of DPDgroup staff who need access to provide services to customer?
	Physical security: DPDgroup UK IT services are hosted in secure controlled data centres within our secure hub sites and off-site data centres. All data centres are monitored 24 x 7 x 52. Access to data centres is further restricted to named individuals via an ID badge system. All DPDgroup UK business locations have high levels of security controlling site access. Data access: DPDgroup Security Access Policy restricts data access to employees based on their role and function ensuring high levels of data security. System access administrators: The DPDgroup IT System Administrator Charter details the rules and practices with which all IT system administrators must comply and is used in addition to the IT User Charter. The Policy incorporates: ● Reference to duties to ensure systems are secure and remain secure ● Responsibility to monitor activities and events to detect potential security incidents ● Bound by confidentiality and non-release linked to their activities ● Only use available authority when required to do so and in line with duties ● A requirement to always document activities, use approved products and report security incidents ● A requirement to collaborate with the BUSO (Business Unit Security Officer) and Data Protection Officer ● Outcome of non-compliance e.g. company disciplinary, civil and criminal penalty
Q7	We send DPDgroup data about parcels, e.g. delivery address, mobile number and email. How is DPDgroup ensuring data security and that the company meets the needs of GDPR?
	In addition to the questions above concerning data security measures for staff, DPDgroup ensures that the security measures taken meet the requirements of GDPR Article 25 (privacy by design and default) and Article 32 (security of data). All data processing principles are based upon GDPR Article 5 (principles of data processing). A. Lawfulness, fairness and transparency B. Purpose limitation C. Data minimisation D. Accuracy E. Storage limitation F. Integrity and confidentiality G. Accountability
Q8	Is DPDgroup planning any changes to data encryption and anonymisation of test data?
	Employee computers are encrypted as standard and databases holding sensitive data are encrypted.

	Due to the nature of the processing of data, extra security controls as stated below in the next question have been deployed.
Q9	What security measures are in place or additional measures planned to meet the requirements of GDPR?
	DPDgroup UK's information security standards are based on its parent company (La Poste) standards which follow the ISO27002 standard and are in accordance with our data protection policies. A nominated individual from the DPDgroup UK IT management team performs the role of Business Unit Security Officer (BUSO) and is responsible for implementing the standards which are jointly agreed with the DPDgroup UK IT Director and other country BUSOs.
Q10	Is DPDgroup transmitting data to us securely?
	For data transfers (scheduled and ad hoc), DPDgroup uses key based SFTP file transfer or HTTPS API. Please contact us at edi.gdpr@dpdgroup.co.uk if you have not completed the move from other less secure methods.
Q11	How does DPDgroup seek consent for the Your DPD App?
	For the processing of data for the Your DPD App, DPDgroup are the controller where data is collected from the consumer, and we are the data processors under Article (6) (1b), where data is given to us by the customer. DPDgroup processing of customer data is needed for the App to work. Customers of the Your DPD App can execute their rights under GDPR following our Data Subject Rights Process.
Q12	How is DPDgroup going to report any data breaches?
	If a personal data breach of security has occurred, it is important that we deal with this promptly and effectively. The breach may arise from a theft, a deliberate attack on our system, the unauthorised use of personal data by a member of staff, accidental loss or equipment failure. However the breach occurs, we must respond to and manage the incident appropriately. In the event of a data breach, we will provide information within 48 hours of being made aware. Our Data Breach Notification Process includes provisions for customer, consumer and ICO (Information Commissioner's Office) notification by our Data Protection Officer.
Q13	How is DPDgroup going to handle requests from its customers to delete, update or correct inaccuracies relating to parcel delivery?
	DPDgroup has a DSAR (Data Subject Access Request) process for each of the six data data subjects' rights and meets the requirements of the ICO (Information Commissioner's Office). Staff are trained on each process, and each request is reviewed by the Security of Information steering group, which meets every six weeks, or, convened immediately in the event of a security incident.
Q14	Can deletion in line with retention periods be maintained, e.g. through automation of deletion or a robust mechanism to ensure ongoing deletion?
	DPDgroup is compliant with the fifth data processing principle and reviews the length of time we keep personal data using the three principles below. ● We consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it. ● We securely delete information that is no longer needed for this purpose or these purposes. ● We update, archive or securely delete information if it goes out of date. There may be a requirement to retain data for longer periods due to regulatory requirements.
Q15	How is DPDgroup improving Data Privacy Impact Assessments (DPIAs)?

DPDgroup already has a defined DPIA process for projects in compliance with GDPR Article 35 where the processing is likely to result in a high risk to the rights and freedoms of the data subjects.

Each DPIA is reviewed at the Business Standards and Governance group, which meets every six weeks or, convened immediately in the event of high risk outcome.

Q16 From which countries is personal data accessed within your organisation?

This is dependent on the service contracted (e.g. whether the delivery is domestic or international). DPD is a member of one of Europe's leading parcels groups, DPDgroup, which is wholly owned by France's La Poste, the second largest postal group in Europe. Data may be shared internationally to support the delivery of parcels and provision of services.

Q17 How DPDgroup ensuring compliance with the GDPR?

To prove GDPR readiness we have had a number of further internal and external audits looking at information security, IT system setup and information (physical and digital) retention and disposal requirements above our normal process. Results are shared with the Business Standards and Governance group to ensure we are prepared and have plans in place for compliance.

Q18 To which countries is data transferred?

This is dependent on the service contracted (e.g. whether the delivery is domestic or international). We always ensure any transfers of data, whether domestic or international, are protected with appropriate adequacy agreements in place with the EU and country of transfer. For example, US companies are signed up to the US/EU privacy shield.

Q19 How long does DPDgroup keep customer data for?

DPDgroup retains personal data no longer than necessary and only for the purposes it was obtained for. We review the length of time we keep personal data using the three principles below.

We consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it; we securely delete information that is no longer needed for these purposes; we update, archive or securely delete information if it goes out of date.

There may be a requirement to retain data for longer periods due to regulatory requirements.

The envisaged time limits for each category are as follows:

- Customer collection requests - 10 months
- Track and trace (parcel tracking) - 10 months
- Shipping data via SFTP gateway - up to 10 days
- Depot operations - 14 days
- Handheld unit - 14 days
- Invoice & credit statements (including name, address of consignee) - 7 years
- All images (including proof of delivery, calling card, consignment notes) - 3 years
- Customer notifications - 3 years (to support claims and losses)

Q20 What do you have within your company relating to security of information and GDPR?

Documents relating to security information and GDPR on page 5

DOCUMENT TYPE	PURPOSE	AUDIENCE
INFORMATION SECURITY POLICY	Overview of how DPDgroup UK ensures reliable, secure and safe use of its IT Systems	Customers Suppliers Partners
IT USERS CHARTER	Rules & practices which all users must comply to ensure reliable, secure and safe use of DPDgroup UK IT Systems and to protect corporate and customer data from security breaches in line with UK Law	All Employees
IT SYSTEMS ADMINISTRATOR CHARTER	Rules & practices which all IT System Administrators must comply to ensure reliable, secure and safe use of DPDgroup UK IT and Communication Systems	IT Administrators
DATA PROTECTION POLICY	Our commitment to protecting personal data, implementation with regards to the collection and use of personal data, to ensure that all DPDgroup employees and contract staff working in DPDgroup offices and under DPDgroup instruction are aware and compliant to the provisions of the GDPR	All Employees
DATA RETENTION & DISPOSAL POLICY	Describes our commitment with regards to the retention and disposal of personal data, awareness and compliant to the provisions of the GDPR	IT Administrators
SUPPLIER DATA OBLIGATIONS POLICY	It sets out DPDgroup UK's minimum expectations and compliance for all suppliers processing DPDgroup Data (known as "supplier data obligations").	Suppliers Partners
PRIVACY (FAIR PROCESSING) POLICY	It explains what happens to any personal data that Consumers provide to us through our Mobile Application or that we collect from consumers who visit our website.	Consumers Website Visitors
SUBJECT ACCESS REQUEST POLICY	The GDPR provides individuals with a right to request access to personal data that a Company holds on them	Consumers Customers Employees
DATA PROCESSING AGREEMENT	This sets out the details of Processing Activities as per the requirements of Article 28 of GDPR	Customers Suppliers Partners