GDPR at DPD

Frequently Asked Questions

Does DPD consider itself to be a data controller and, if so, what are the implications?

Yes - under GDPR, DPD will be controller for all data we collect ourselves, and processor for the majority of our customers' data. We will have the same obligations as a controller or processor under GDPR to handle personal data correctly - only retaining data for as long as required in order to conduct our business, and securing the data we hold subject to our retention policy.

We send DPD data to enable the parcel, e.g. delivery address, mobile number and email. How is DPD ensuring its security and that it meets the needs of GDPR?

At DPD UK we understand the importance of having a robust, well-defined structure with supporting processes and principles to successfully manage and secure the technology we utilise and provide. That is why it forms part of our overall management strategy. We have implemented a governance framework which ensures accountability for our Information Security Policy.

Everybody who works for the company must acknowledge responsibility for and understand the importance of maintaining the security of customer, employee and other confidential information.

We build 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.

We will continue to monitor and meet the requirements of legislation, to provide assurance that our information protection is appropriate for our business and identify security solutions that are tailored for DPDgroup UK business requirements to support customers and our employees.

Our Security of Information Steering Group already meets every six weeks on standards on our dashboards, Privacy Impact Assessments (PIAs), Subject Access Requests, Lost Equipment and any Data Breaches and information security issues.

How is DPD improving Privacy Impact Assessments?

Today we are compliant with the Data Protection Act, and completion of PIAs is part of our current project management process. We are now widening this to perform PIAs as part of any change to our systems involving personal data.

How is DPD going to handle requests from its customers to delete, update or correct inaccuracies relating to their data?

We already have a process in place to delete parcel recipient data on request. Changes to consignment details are the responsibility of the customer where we are a data processor.

Is DPD planning any changes to data encryption and anonymisation of test data?

We are investigating the type of encryption the data at rest on servers has as well as the anonymisation of test data relative to the categories of data stored, the nature of our processing activities and design and functionality constraints. As a compensating control we have an additional set of firewalls from the corporate network that is present on a different network from the other services between corporate and database as well as complex network segmentation.

Is DPD transmitting data to us securely?

Actually, we may need you to change! Going forward, all data communications will be via secure FTP (SFTP), specifically if you are an EDI customer. If your communications need to change, we will be in touch shortly.

How is DPD going to report any data breaches?

In order to comply with GDPR, our DPO will report any data breaches to the ICO (and to the Security team) and / or our customers (where relevant) without undue delay.

How does DPD seek consent for the YourDPD app?

When you download and use the app consent is collected.

How does DPD ensure that suppliers it passes data onto are compliant with GDPR?

We currently require all processors and sub-processors of DPD who process personal data to agree to our Supplier Data Obligations Policy.

We are now working with our legal advisors to update our Supplier Data Obligations Policy and all of our supplier contracts to ensure these are all compliant with GDPR. We will obtain written confirmation from all of our suppliers as GDPR comes into force.

Can DPD delete all personal data outside a retention period prior to 25 May 2018?

Yes we can where there is a legal requirement, although there may be circumstances where we need to keep the data, in the event of a claim or dispute or if the data is used for a purpose that relies on retaining it. In most cases the parcel data is one-off data that is only a point-in-time record and is kept for a fixed period to support accounting, analytics and responding to complaints.

Can deletion in line with retention periods be maintained, e.g. through automation of deletion or a robust mechanism to ensure ongoing deletion?

Yes it can, and we are currently reviewing our Data Retention & Disposal Policy to ensure we remain compliant.

Is access to personal data restricted to members of DPD staff who need access to provide services to customer?

Yes, we have robust access control restrictions on all systems.

Can DPD retrieve personal data relating to a specified parcel recipient and provide a copy within 10 days of receiving a request from a customer?

Yes.

Can DPD correctly identify inaccuracies in an individual's data within 10 days of receiving a request from a customer?

Yes.

Can DPD permanently delete personal data relating to a specific individual within 10 days of receiving a request from a customer?

Yes.

Are there any other organisations (either within your group company or wider vendor community) who you are, or anticipate you will be, sharing our personal data with as a sub-processor?

Yes, we will share personal data with different organisations, dependent on the service applicable (either to deliver parcels or additional services). All of our sub-processors have completed a Supplier Data Obligations Policy document which requires they adhere to GDPR.

What processing operations are being undertaken on the personal data (e.g. capturing directly from the individual, collecting from an external source, collecting from an internal source, storing, transferring internally, transferring externally, updating, manipulating, duplicating or copying, deleting)?

We capture, store and transfer data internally in order to fulfil the service contracted. Once the service has been satisfactorily completed, the data will be deleted.

We may also perform further processing activities on personal data if requested by a customer, such as in relation to correcting inaccuracies or retrieving copies of personal data.

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 across the EEA to support the delivery of parcels.

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 safeguards and contractual controls, e.g. Privacy Shield.

Which of your suppliers support the system and/or have the ability to access personal data on the system?

This is dependent on the service contracted. We always ensure any transfers of data, whether domestic or international, are protected by appropriate safeguards.

How do you ensure that the accuracy of personal data is maintained?

If the data is used for a purpose that relies on keeping it current it will be kept up to date. In most cases the parcel data is one- off data that is only a point-in-time record and is kept for a fixed period to support accounting, analytics and responding to complaints, which may defeat the point of us keeping it up to date.

Do you have data segregation capability?

Due to the nature of our business and intentional system design, the data we are given is not separated out, either logically or physically.