ONEPOST's commitment to the General Data Protection Regulation (GDPR)

Version November 2017

Commitment Statement

The EU GDPR is due to come in to operation on the 25th May 2018. This replaces the existing 1995 EU Data Protection Directive, and will enhance the rights EU individuals have over their data. GDPR will create one law, ensuring a uniform approach to data handling across Europe.

ONEPOST is committed to comply with the GDPR regulations as a Data Controller and Processor, and is currently undertaking a number of steps to achieve this. We are working closely with the ICO (Information Commissioner's Office) and the DMA (Direct Marketing Association) to ensure that we comply for all data we handle, including customers, suppliers, our CRM and Employee Data.

ONEPOST is also looking at its own service offerings to help our customers meet the new regulations through Data Retention and Transit.

What ONEPOST are doing?

At ONEPOST we have a working party made up of various experienced members throughout the Business. These members are looking closely at each paper that is released by the ICO to ensure we are doing everything needed to comply in readiness for 25th May 2018.

As a Data Processor

Where ONEPOST is the Data Processor for our customers, and Data Controllers, we take great care of data to ensure that any responsibilities are managed to minimise any risk to any data.

Third-party Audit and certifications

ONEPOST holds ISO certification for the following standards, ISO 9001, ISO14001 and ISO27001. We undergo a full internal and external annual audit to achieve these certifications. This audit covers all aspects of our data security and procedure management. Including but not restricted to the following key controls:

- **Access control and Management**
- **Corporate Governance**
- **Data security, retention and backup**
- **Change Management**

In addition, ONEPOST are regularly audited by our clients to ensure compliance with their exacting security standards which often exceed the regulations.

What a Data Controller should do next?

There are a number of things to consider if you are a Data Controller and looking to prepare yourselves for the GDPR introduction.

Get to know GDPR

Information relating to the GDPR is readily available from the ICO online, www.ICO.org.uk . This includes a guide, ***"12 Steps to take now"***, that covers the following 12 areas of concern and will help any company understand their starting point:

- Awareness
- Information you hold
- Communication
- Individuals Rights
- Subject Access requests
- Lawful basis for processing personal data
- Consent
- Children
- Data Breaches
- Data Protection by design and data Protection Impact Assessments
- Data Protection Officers International.

Auditing your data

Consider looking at your data inventory with a view to review and update the information you control. Assess that these are adequate and plan how to address any gaps. During this you may also wish to review your process documentation and the lawful basis for processing. You may wish to conduct an exercise to carry out a maintenance check on your data. ONEPOST can help you with Data Cleansing should this is be a service you would find useful.

International Transfers of Data

Where Personal data is being transferred to a processor outside the EEA the Data Controller must have a "Controller to Processor" contract in place.

What is Next?

The Government has confirmed its plans to introduce a Data Protection Bill to Parliament and this should become law in 2018 replacing the current Act. It will:

- Set out derogations from the GDPR, ie areas where Member States can decide provisions, such as around some exemptions
- Contain other national implementing measures, such as the Commissioner's powers
- Implement the Law Enforcement Directive, which covers processing by competent authorities such as police forces for law enforcement purposes
  Cover those areas of data processing that are not covered by either GDPR or the Directive and are outside the scope of EU law, so that there will be no gaps in the UK's data protection regime.