

# Data Protection Policy

## Print4UK Limited 2011

### Background

In the arena of digital printing, Print4UK handles personal data supplied by clients. This data is confidential and is used only for the purpose of producing that particular personalised digital printing project. This personal data may include names and addresses of individuals and companies.

As such, Print4UK has a duty of care under the data protection legislation, to define, implement and enforce a data protection policy which protects the confidentiality of such data on our computer systems. This policy provides details of our data handling arrangements.

### Print4UK Operations

Print4UK Limited operates from 2 sites in North East London.

### Firewall Security

To ensure it is effective in its role, the Print4UK firewall is managed and maintained on a regular basis. The network is connected to the internet through a high security firewall router, providing and enforcing perimeter security to the network, and preventing unauthorised access and intrusion.

### External Access Security

Access to the Print4UK network for the purpose of IT support and working is secure and uses either IPSec VPN or SSL encrypted HTTP access.

### Internal Security

Access to all PCs/Macs and servers is password protected. Passwords are confidential to Print4UK Limited Directors and technical support staff. No passwords are kept in written or electronic form.

### Other Security

Access to Print4UK premises is carefully controlled during working hours. Outside of normal working hours the premises is secured via locked gates and 24 hour CCTV.

### Protecting the Client-Supplied Data

Clients data include names and addresses of individuals and companies. This data is supplied to Print4UK for the purpose of producing printed materials specific to individual companies, which are then delivered by Print4UK Limited as fulfillment of orders.

The control of data is managed from entry onto the infrastructure to the point of either deletion from Print4UK servers or secure archival. To handle the sensitive data and comply with Data Protection regulations Print4UK utilises the following security measures.

## **Supply of Data to Print4UK by Clients**

Data that is supplied electronically (either as an email attachment or an electronically transferred file) should be password protected or encrypted by the client, and that the passwords and decryption keys be communicated to Print4UK over the telephone or text message. Print4UK undertakes to keep unlocking and decryption passwords in non-electronic form and separate from the client supplied data.

## **Data on the Print4UK Servers**

Print4UK stores sensitive data only for the duration of the digital print process in an encrypted format.

## **Control and Handling of Data**

During the data merge stage of the digital print process, the sensitive data is handled in encrypted form and deleted upon completion. Systems ensure that there is no trace of data in encrypted form.

## **On Completion, Archiving or Disposal**

On consultation and with prior agreement from the client, the data is either archived in secure format or is permanently removed and deleted. All data that is archived will remain encrypted. Only authorised Print4UK personnel or technical support staff are able to restore archived data.

*We will review this policy on a regular basis.*

*Print4UK Limited 2011*