CRYSTAL BUSINESS PRINT LTD
DATA SECURITY AND DATA PROCESSING POLICY

ICO Registration: ZA055793

Crystal Business Print Ltd is a printing and direct mail company. Our customers send us mailing lists which we use to produce personalised mailings on their behalf.

System Security

- Only authorised staff have access to the network where personal data is stored;
- All waste paper which might contain sensitive information (e.g. misprints) will be placed in a designated bin and removed by our contractor for secure destruction;
- Our network is protected by a firewall, anti-virus software, email filtering system, all of which are kept up-to-date;
- All PCs kept fully updated and password protected

Incident Management

Any and all incidents must be reported immediately in the first instance to the Data Manager. If we become aware of a data breach, we will contact the data controller within 24 hours.

Physical Security

- All visitors are required to report to the office and sign in and out of building.
- Gate padlocked; all external doors locked each evening, and further protected by lockable roller shutters.
- There are also 2 internal doors which are locked and protected by a roller shutter. Only directors and senior managers have access to keys.
- The premises are protected by a monitored burglar alarm.

Data Transfers

We will always use secure methods to transfer data, and we encourage our customers to do the same. We will not use any service provider who may store or process data on servers outside the EU.

Data Processing and Retention

Customers supply us with personal data in the form of mailing lists which we use to produce personalised mailings on their behalf, so that they can pursue their legitimate business interests and communicate important information to their customers, members or other interested parties.

We encourage our customers to ensure that personal data that they send to us for mailing purposes is correct, up-to-date and relevant.

We will only process mailing lists in accordance with our customers' written instructions.

We will use mailing lists only for the purposes for which they have been supplied, and we will not share them with anybody without written instructions from our customers.

When a mailing is completed, we will retain the mailing list for a maximum of 90 days so that we can investigate any customer queries that arise. We will then securely delete the data from our network.

Rights of Data Subjects

Data subjects have the following rights:

- the right to request a copy of personal information held about them;
- the right to request that inaccuracies be corrected;
- the right to request us to stop processing their personal data;
- the right to withdraw consent.

Upon request from our customer or the data controller, we will assist them in facilitating the assertion of the above rights by data subjects whose personal information is contained within data supplied to us by our customer or by the data controller.

We also have access to 3rd Party software which can be used to assist in protecting the rights of data subjects before a mailing is produced. Examples of this could include:

- PAF cleansing and Goneaway screening, which can be used to correct inaccuracies.
- Mailing Preference Service screening, which can be used to help protect the right of data subjects to withdraw consent.

While the use of the above services may not be appropriate in every case, we strongly recommend that our customers consider using them to help ensure that their mailings comply with the GDPR.

Customer Data

When our customers contac us by telephone or email, we will store their email addresses and/or telephone numbers so that we can contact them to discuss the services that we provide for them. We will attempt to keep this contact information as accurate as possible, and we will be happy to delete or correct the contact details of any customer upon receiving their written request.