	TITLE	QUALITY MANAGEMENT SYSTEM DOCUMENT
BLUEPRINT	**GDPR STATEMENT**	**BP 5020 B**

Blue Print Management Services Ltd (trading as Blue Print Direct Mail) will use the following statement to secure and monitor the personal data that it holds and processes. Blue Print Direct Mail is an ISO 27001 accredited company, and as such all new staff are trained in dealing with personal data during their induction. Existing staff have also received training, and where their role deems it necessary, this training is ongoing.

All personal data held by Blue Print Direct Mail is stored securely by one of following methods.

Physical paper records are stored in a cabinet located in the Managing Director's office. This is locked at all times when not in use, and there are only 2 key holders, Anthony Drew (MD) and Sue Law (Accounts & HR). All digital records are stored on a specific partition on the company server, located at our business premises, and access is restricted to specific personnel by a password. These digital documents are also password protected as a secondary level of security. Paper documents containing personal data that are no longer required are disposed of in our secure waste bins located in the production department or shredded in the office. When personal data of employees needs to be sent off-site, for example to our accountants, this has been agreed to by employees as part of their Contract of Employment, and details are always treated sensitively and discretely. Copies of Employee Contracts are held by Anthony Drew (MD).

At present we only market our services to businesses, not the public. However, if this changes we will update this accordingly to comply. If any business should request that they no longer wish to receive marketing material, they will be removed from our mailing list.

For the purposes of security and crime prevention, we do have CCTV cameras on our premises, both inside and out. Signage is displayed at both front and rear entrances informing everyone of this and detailing ways they can contact the scheme operator should they have any issues. Cameras are positioned so that they only capture images relevant to security and crime prevention, and have as little impact on the general public as possible. The recording equipment is kept in a locked server cabinet to prevent unauthorised access, and is located in an access-restricted area of the premises.

Data supplied to Blue Print Direct Mail for the purposes of direct mail printing and fulfilment is treated in a slightly different way, as we do not source this ourselves. Although we may not be responsible in the harvesting of this data, we still take the responsibility of handling our client's data very seriously. We advise that all our customers submit their data to us via a secure, encrypted connection service and we offer this service free of charge. Once the data is downloaded, it then resides on a dedicated partition of the company server to which access is restricted. Only the employees that require it to complete their tasks will have access to this partition and the data held within. All proofs that contain personal information are password protected. Data that is submitted to us resides on our server for 3 months only, and is then deleted.

Customers are always advised to have a data cleanse performed prior to mailing, and we offer a free of charge audit and estimate. At this stage our client can request that their data be run against MPS.

Printed items that contain personal data are disposed of in secure waste bins which are kept locked at all times. This waste is then securely shredded on-site and documentation of this is kept by Anthony Drew (MD).

Signed: …… **……**

Philip Morris
Operations Manager