

## GDPR PROCEDURES

Data Protection Officer will adhere to the following:

### 1. Definitions

- a. 'the controller' Client
- b. 'the processor' Jump Design & Print Ltd
- c. 'sub-contractor' Supplier
- d. 'Data protection officer' Nathan Bendall

### 2. Handling Data

- a. On receipt of order the processor will provide an online encrypted secure password-protected file transfer to the controller <https://jumpdpwettransfer.com>
- b. In the event the controller cannot gain access it will be the controller's responsibility to send the data via an encrypted source/link.
- c. On receipt of link, once clicked the controller will receive an email confirmation for receipt of delivery
- d. Once data has been transferred to the processor's secure server the files will be password protected
- e. Approval/Amend of any data proofs will be sent to the controller via the online encrypted secure password-protected file transfer
- f. On completion of order data will be held up to 14 days with a maximum of 28 days on the processors secure server
- g. All processes/actions to be documented by the data protection officer
- h. With all processes/actions the processor can only act on the written instructions of the controller

### 3. Request for Access

- a. Request for access will need to be submitted by written confirmation to the data protection officer
- b. On receipt of request the processor will notify the controller, on written instructions of the controller the Data protection officer will assist.

### 4. Data Breaches

- a. In the case of a personal data breach, the processor shall notify the controller without undue delay after becoming aware of a personal data breach
- b. The notification will describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- c. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- d. describe the likely consequences of the personal data breach;
- e. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects
- f. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without und further delay
- g. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.