



# Data Protection Policy

## **1. ABOUT THIS POLICY**

2. Creative62 ("we") are committed to protecting and respecting your privacy through data protection. We can be contacted at enquiries@creative62.com or 0116 275 2831 please speak to Mark Robinson
- 2.1 You are obliged to comply with this Policy when processing personal data on our behalf. Any breach of this Policy may result in disciplinary action. We reserve the right to change this Policy at any time.

## **3. OVERVIEW**

- 3.1 "Personal data" means any information relating to an identified or identifiable natural person (i.e. a "data subject"). In particular, we are legally obliged to ensure the following:
  - 3.1.1 that we process personal data in a fair, lawful and transparent manner;
  - 3.1.2 that we collect personal data for specified, explicit and legitimate purposes;
  - 3.1.3 that we ensure that personal data is adequate, relevant and limited to what is necessary;
  - 3.1.4 that personal data is only transferred to a third party processor if it agrees to comply with our procedures and policies, or if it puts in place adequate measures in accordance with the relevant data protection legislation in the UK;
  - 3.1.5 that we keep personal data up to date and take steps to ensure the accuracy of the personal data we hold, erasing or rectifying any inaccurate data without delay;
  - 3.1.6 that we keep personal data for no longer than is necessary;
  - 3.1.7 that we take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or destruction or damage to, personal data; and
  - 3.1.8 that we put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

## **4. FAIR, LAWFUL AND TRANSPARENT PROCESSING**

4.1 For personal data to be processed lawfully, it must be processed on the basis of one of a number of specified legal grounds, which may be summarised as follows:

- 4.1.1 the data subject has provided their consent;
- 4.1.2 the processing is necessary for the performance of a contract, or entering into a contract;
- 4.1.3 the compliance with a legal obligation;
- 4.1.4 the processing is necessary in order to protect the vital interests of the data subject or another natural person;
- 4.1.5 the processing is necessary for the performance of a task carried out in the public interest; or
- 4.1.6 in the pursuit of our legitimate interests, where we have told the data subject what these interests are. This does not apply where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4.2 We shall only process personal data for the specific respective purposes set out in Schedule 1 or for any other purposes specifically permitted by the relevant data protection legislation. We shall notify those purposes to the data subject when we first collect the data.

## **5. NOTIFYING DATA SUBJECTS**

5.1 If we collect personal data directly from data subjects, we must inform them, at the point in which we collect the data, of:

- 5.1.1 our identity and contact details;
- 5.1.2 the purposes for which we intend to process the personal data as well as the lawful basis for processing;
- 5.1.3 if the processing is in the pursuit of our legitimate interests, what these interests are;
- 5.1.4 the recipients or categories of recipients of the personal data, if any;
- 5.1.5 if applicable, the fact that we intend to transfer personal data to a third country;
- 5.1.6 the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- 5.1.7 the existence of their data subject rights;

- 5.1.8 the existence of the right to withdraw consent at any time (where the processing is based on the customer's consent), without affecting the lawfulness of processing based on consent before its withdrawal;
  - 5.1.9 the right to lodge a complaint with a supervisory authority;
  - 5.1.10 whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and
  - 5.1.11 if applicable, the existence of any automated decision-making process which we intend to use in connection with the personal data, including profiling.
- 5.2 If we receive personal data about a data subject from other sources, we should provide the data subject with the above information as soon as possible after we have received it, and in any event no later than one month from when we first received the data, or the date on which the data is first used (whichever occurs first).

## **6. PROCESSING IN ACCORDANCE WITH DATA SUBJECT'S RIGHTS**

- 6.1 We shall process all personal data in accordance with the rights of the data subject, in particular their right to:
- 6.1.1 request a copy of the information we hold about them ("Access Request");
  - 6.1.2 request that we rectify any information we hold about them ("Right to Rectification");
  - 6.1.3 request that we erase any information we hold about them ("Right to be Forgotten");
  - 6.1.4 restrict the level of processing we carry out with the information ("Restriction of Processing");
  - 6.1.5 obtain from us all personal data we hold about them, in a structured, machine readable form, and have this information transmitted to another organisation ("Data Portability");
  - 6.1.6 object to processing their personal data in certain ways ("Right to Object"); and
  - 6.1.7 withdraw their consent at any time to receiving marketing communications from us ("Right to Withdraw Consent").

- 6.2 Employees who receive a written request of any of the kinds mentioned above must forward it to Mark Robinson immediately who will be able to respond to the request in a timely and appropriate manner. We must not refuse to act on any request of the data subject to exercise his or her rights unless we can clearly demonstrate that we are not in a position to identify the data subject.

## **7. DISCLOSURE OF PERSONAL INFORMATION**

- 7.1 We must only share and disclose personal information in the manner set out in this Policy, in particular Schedule 1, unless we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, in order to enforce or apply any contract with the data subject or other agreements, or, to protect the vital rights of the data subject, our employees, customers, or others.

## **8. TRANSFERRING PERSONAL DATA TO A THIRD COUNTRY OUTSIDE THE EEA**

- 8.1 We may only transfer any personal data we hold to a country outside the European Economic Area ("EEA") if one of a number of specific conditions applies, namely if:
- 8.1.1 the European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;
  - 8.1.2 appropriate safeguards are in place, such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism;
  - 8.1.3 the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks;  
or
  - 8.1.4 the transfer is necessary for one of the other reasons set out in the relevant data protection legislation.
- 8.2 If you intend to transfer personal data outside of the EEA, please consult Mark Robinson who will assist you with this process to ensure that the data is being transferred lawfully.

## **9. DATA RETENTION**

- 9.1 We must ensure that personal data we hold is accurate and kept up to date. We shall check the accuracy of any personal data at the point of collection and at regular intervals afterwards, and in any event we should perform a review to this effect no later than the time periods specified in Schedule 1. We shall take all reasonable steps to destroy or amend inaccurate or out-of-date data whenever this comes to our attention.

## **10. DATA SECURITY**

- 10.1 We shall maintain data security by testing and protecting the confidentiality, integrity, availability and resilience of the personal data, in the following ways:
- 10.1.1 All day-today personal data and company records are sorted onsite via password protected software. All communication devices are password protected. All third party or cloud-based services used for commercial purposes have been confirmed as secure.

## **11. DATA BREACHES – IMMEDIATE STEPS TO TAKE**

- 11.1 A "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. In the case of a personal data breach, you must:
- 11.1.1 try to contain the breach and limit its scope and impact, for example, by telling the recipient to destroy, remove and not discuss the information; and
- 11.1.2 immediately inform Mark Robinson of the breach, including as much information as possible such as the date and time of the breach, when it was detected, who committed the breach, how many data subjects were involved, and any measures already taken to try and contain the breach.
- 11.1.3 [ANY OTHER STEPS]
- 11.2 Upon receipt of the notification above, Mark Robinson shall, without undue delay and not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioners Office. Where the notification to the Information Commissioners Office is not made within 72 hours, the notification must be accompanied by reasons for the delay.

## 12. DATA BREACHES – WHEN TO NOTIFY THE DATA SUBJECT

12.1 We are only required to notify the personal data breach to the data subject where it is likely to result in a high risk to their rights and freedoms. This must be done without undue delay and describe in clear and plain language the nature of the breach.

### SCHEDULE 1- DATA PROCESSING ACTIVITIES

Item No	Type of data subject	Type of data	Type of processing	Purpose of processing	Retention Period
1	Client record	Contact details	Addition and update on File Maker our in-house CRM	Addition and update on File Maker our in-house CRM	Duration of working relationship
2	Invoice details	Book Keeping	Book Keeping	Book Keeping	Duration of working relationship
3	Accounts	Transfer to Xero	Book Keeping	Book Keeping	Duration of working relationship
4	Accounts	Yearly Accounts	Accounts	Accounts	Duration of working relationship or for six years as accounts record.
5	Account back-up	PDF	Back-up of monthly invoices to Dropbox	Back-up of monthly invoices to Dropbox	Duration of working relationship or for six years as accounts record.