Data Protection Policy | Troy Planning + Design

Table of Contents

This Policy has been approved and authorised by:

Name:	Troy Hayes
Position:	Managing Director
Date:	24 May, 2019
Due for Review by:	24 May, 2020

Section A: Overview

1. The reason for this policy

1.1 You have legal rights with regard to the way your personal data is handled.

1.2 In the course of our business activities we collect, store and process personal data about our customers, suppliers and other third parties, and therefore in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful treatment of this data.

1.3 All people working in or with our business are obliged to comply with this policy when processing personal data.

2. Introduction

2.1 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, for example, customers and business contacts, or that is provided to us by data subjects or other sources.

2.2 It also sets out our obligations in relation to data protection under the General Data Protection Regulation ("the **Regulation**").

2.3 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.4 The procedures and principles set out herein must be followed at all times by us and our employees, agents, contractors, or other parties working on behalf of the Company.

2.5 We aim to ensure the correct, lawful, and fair handling of your personal data and to respect

your legal rights.

3. The meaning of key Data Protection terms

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy includes all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4. Summary of the Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) **(Processed fairly and lawfully)** processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) **(Processed for limited purposes and in an appropriate way)** collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) **(Adequate, relevant and not excessive for the purpose)** adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) **(Accurate)** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) **(Not kept longer than necessary for the purpose)** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;

f) **(Processing in line with data subject's rights)** personal data must be processed in line with data subjects' rights, in particular your right to:

4.1.1 request access to any data held about them by a Data Controller (see also clause 15).

4.1.2 prevent the processing of their data for direct-marketing purposes.

4.1.3 ask to have inaccurate data amended (see also clause 9).

4.1.4 prevent processing that is likely to cause damage or distress to themselves or anyone else.

g) **(Security)** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

h) **(Transfers outside EEA)** not transferred to people or organisations situated in countries without adequate protection.

5. Our use of personal data and our purpose

We collect, hold, and process the personal data referred to in Schedule 1 (and the purpose for which we process that personal data is also set out in Schedule 1).

6. Our data protection measures

When we are working with personal data we take **t**he measures set out in Schedule 2.

Section B: Data Protection Principles

7. Lawful, Fair, and Transparent Data Processing

The Regulation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The processing of personal data is lawful if one (or more) of the following applies:

a) **(consent)** the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) **(contract)** processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c) **(legal obligation)** processing is necessary for compliance with a legal obligation to which the Data Controller is subject;

d) **(protection)** processing is necessary to protect the vital interests of the data subject or of another natural person;

e) **(public interest)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller;

f) **(legitimate interests)** processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

8. Processed for Specified, Explicit and Legitimate Purposes

8.1 The Company collects and processes the personal data set out in Schedule 1 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and can include data received from third parties.

8.2 The Company only processes personal data for the specific purposes set out in Schedule 1 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

9. Adequate, Relevant and Limited Data Processing

9.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 5, above.

10. Accuracy of Data and Keeping Data Up To Date

10.1 The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. Timely Processing

11. The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

12. Secure Processing

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

12.1 An assessment of the risks posed to individual data subjects; and

12.2 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

Section C: Data Subject Rights

13. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;

b) The right of access;

c) The right to rectification;

d) The right to erasure (also known as the ‘right to be forgotten’);

e) The right to restrict processing;

f) The right to data portability;

g) The right to object;

h) Rights with respect to automated decision-making and profiling.

14. Keeping Data Subjects Informed

14.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the Company including, but not limited to, the identity of Sue Mulcaster, its Data Protection Officer;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Schedule 1 of this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 26 of this Policy for further details concerning such third country data transfers);

g) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

h) Details of the data subject's rights under the Regulation;

i) Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

14.2 The information set out above in Part 14.1 shall be provided to the data subject at the following applicable time:

14.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;

14.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication; or

b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c)In any event, not more than one month after the time at which the Company obtains the personal data.

15. Data Subject Access

15.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases, the data subject shall be informed of the need for the extension).

15.2 All subject access requests received must be forwarded to Sue Mulcaster the Company's data protection officer smulcaster@troyplanning.com.

15.3 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

16. Rectification of Personal Data

16.1 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

17. Erasure of Personal Data

17.1 Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c)The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 20 of this Policy for further details concerning data subjects' rights to object);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

17.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

17.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

18. Restriction of Personal Data Processing

18.1 Data subjects may request that the Company ceases processing the personal data it holds about them.If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

18.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

19. Data Portability

19.1 The Company processes personal data using automated means. Such as analytics from MailChimp.

19.2 Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other Data Controllers, e.g. other organisations).

19.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following formats: CSV and Excel spreadsheet.

19.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another Data Controller.

19.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

20. Objections to Personal Data Processing

20.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistical purposes.

20.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

20.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

20.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistical purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

21. Automated Decision-Making

21.1 In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

21.2 The right described in Part 21.1 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;

b) The decision is authorised by law; or

c)The data subject has given their explicit consent.

22. Profiling

22.1 Where the Company uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

Section D: Our Other Obligations

23. Accountability

23.1 The Company's data protection officer is Sue Mulcaster: smulcaster@troyplanning.com

23.2 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the Company, its data protection officer, and any applicable third party Data Controllers;

b) The purposes for which the Company processes personal data;

c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;

d) Details (and categories) of any third parties that will receive personal data from the Company;

e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

f) Details of how long personal data will be retained by the Company; and

g) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

24. Privacy Impact Assessments

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

24.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

24.2 Details of the legitimate interests being pursued by the Company;

24.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

25. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;

i) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

26. Transferring Personal Data to a Country Outside the EEA

26.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

26.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority

(e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) The transfer is made with the informed consent of the relevant data subject(s);

d) The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

e) The transfer is necessary for important public interest reasons;

f) The transfer is necessary for the conduct of legal claims;

g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

27. Data Breach Notification

27.1 All personal data breaches must be reported immediately to the Company's data protection officer.

27.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

27.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 27.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

27.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c)The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

28. Implementation of Policy

28.1 This Policy shall be deemed effective as of 24th May, 2018.No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Schedule 1: Our Use Of Personal Data And Our Purpose

The following personal data may be collected, held, and processed by the Company:

a) Personal contact information (First and Last names, address, phone number, email and website) for communication purposes.

b) Bank account/sort code numbers in relation to accounts payable and disbursements in relation to Invoicing.

Schedule 2: Our Specific Data Protection Measures

These are the measures we take when working with personal data:

a) All emails containing personal data must be encrypted using Google Apps encryption.

b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hard Copies should be shredded, and electronic copies should be deleted securely.

c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

g) Where Personal data is to be transferred in hard copy form it should be passed directly to the recipient;

h) No personal data may be shared informally and if an employee, agent, subcontractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Sue Mulcaster (Office Coordinator): smulcaster@troyplanning.com;

i) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Sue Mulcaster (Office Coordinator): smulcaster@troyplanning.com;

k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

l) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of Sue Mulcaster (Office Coordinator): smulcaster@troyplanning.com and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

n) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other

parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

o) All personal data stored electronically should be backed up annually with backups stored on company hard drives AND/OR cloud services, such as Dropbox or Google Drive. All backups are encrypted as following: Dropbox encryption uses 256-bit AES keys to protect files at rest, and encrypts data in motion with 128-bit AES SSL/TLS encryption or better. Google Drive files in motion are protected using 256-bit SSL/TLS encryption, while those at rest are encrypted with 128-bit AES keys.

p) All electronic copies of personal data should be stored securely using passwords and data encryption as specified at point ***o)***;

q) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;

r) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

w) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Sue Mulcaster (Office Coordinator): smulcaster@troyplanning.com to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually.