

## **DEFINITIONS**

The Design Office:	Partnership comprising Rebecca Austin (nee Bacon) and Selina Austin trading in the UK as 'The Design Office'
Workers:	Employees and Sub-contractors
Third Parties:	Includes, but not restricted to Business Contacts, Clients, Client Referrers and Suppliers
Data:	For the purpose of this document Data means personal data or information which relates to a living person who can be from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data. It may include but is not exclusively restricted to contact details and date of birth, bank details and information in relation to tax status including national insurance number, identification documents including passport and driving licence and other information, an agreement with us, images (whether captured on CCTV, by photograph or video);
GDPR:	The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.
Data Controller:	The entity that determines the purposes, conditions and means of the processing of personal data
Data Protection Officer (DPO):	An officer of The Design Office who is responsible for ensuring that we are adhering to the policies and procedures set forth in the GDPR
Data Subject:	A natural person whose personal data is processed by a controller or processor
Processing:	Any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.
SAR:	Data subjects can make a 'subject access request' to find out the information we hold about them.
Subject Access Right:	Also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

# 2018 ACT: THE DATA PROTECTION ACT 2018

## OVERVIEW

The Design Office takes the security and privacy of data seriously. We need to gather and use information or 'data' as part of our business and to manage our relationships. We intend to comply with our legal obligations under the 2018 Act and GDPR in respect of data privacy and security. We have a duty to notify a data subject of the information contained in this policy.

The Design Office has measures in place to protect the security of data in accordance with our Data Security Policy. The Design Office will hold data in accordance with our Data Retention Policy. The Design Office will only hold data for as long as necessary for the purposes for which we collected it. The Design Office is a 'data controller' for the purposes of data held by The Design Office.

This policy explains how The Design Office will hold and process Data and explains the rights of data subjects. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, The Design Office intends to comply with the 2018 Act and the GDPR.

## DATA PROTECTION PRINCIPLES

Data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

This policy applies to all Data whether it is stored electronically, on paper or on other materials. Data might be provided to us by data subjects, or someone else (such as a Business Contact).

'Processing' means any operation which is performed on data such as:

- collection, recording, organisation structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing data which forms part of an electronic filing system and any automated processing.

## HOW WILL WE PROCESS YOUR DATA?

We will use your Data for:

- complying with any legal obligation; or
- if it is necessary for our legitimate interests.

However, we can only do this if your interests and rights do not override ours. You have the right to challenge our legitimate interests and request that we stop this processing. See details of your data subject rights below.

We can process Data for these purposes without the knowledge or consent of the data subject.

We will not use Data for an unlawful purpose.

If you choose not to provide us with certain Data you should be aware that we may not be able to carry out certain

parts of the contract between us. For example, if you not provide us with the necessary FTP information, we will not be able to make updates to your website or without the relevant company information, prepare an annual report or brochure on your behalf.

Some examples (but not necessarily an exhaustive list) of when we might process your Data;

We are required to process your Data in various situations to carry out the contract between us and to enable us to trade with you, for example (but not limited to) to provide domain hosting and management services, website hosting, website updates, layout for print (Annual Reports for example), strategic marketing and other professional services on your behalf.

### **OUR OBLIGATIONS AS A DATA PROCESSOR ARE;**

- we will only act on the documented instructions from you, the client (the controller)
- we will not share sensitive data with a sub-processor without consent from you
- we will keep records of our processing activities on your behalf
- we will notify you if a breach occurs
- we will co-operate with the regulator i.e. the Information Commissioner's Office (ICO)
- we will monitor our compliance and that of others with our policies and our contractual obligations;
- the prevention and detection of fraud or other criminal offences;
- for any other reason which we may notify you of;
- complying with our legal obligations of whatsoever nature

### **DATA PROTECTION IMPACT ASSESSMENT**

This may be carried out by The Design Office for any new projects where the processing of sensitive data is required as part of our contractual agreement.

### **SHARING YOUR DATA**

Whatever the nature of your relationship with The Design Office we may share your Data with workers, sub-contractors and relevant third parties to carry out our contractual obligations, or for our legitimate interests.

We require those recipients to keep your Data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

- We will not share Data informally.
- We will keep Data secure and not share it with unauthorised people.
- We will regularly review and update Data which we have to deal with for our work.
- We will not make unnecessary copies of Data and will keep and dispose of any copies securely.
- We will use strong passwords as required by our Data Security policy and Mobile Device Policy.
- We take necessary precautions to protect data by securing access to systems whilst not in use, as required by our

### **DATA SECURITY POLICY AND MOBILE DEVICE POLICY.**

- All Data is held securely in line with GDPR requirements;
- We do not store Data on personal computers or other mobile devices for longer than is necessary to process the information.
- We do not store Password or Account details in the Cloud. Sensitive and regulated Data is stored in Password Protected files with XTS-AES-128 encryption with a 256-bit key encrypted. We do not keep back ups of your Data - as data controller, you should maintain backups of your Account information and update passwords regularly to protect and secure your accounts. Where we may set passwords on your behalf - we will only set Strong Passwords (min 12 characters/ to include upper and lower case letters, special characters and numbers)

Data is never transferred outside the European Economic Area, except in compliance with the law and under authorisation of the Data Protection Officer and consent of the data processor.

Printed data is shredded and disposed of securely when finished with, in compliance with our Data Security Policy

Our workers will ask for help from our Data Protection Officer if they are unsure about data protection or if they notice any areas of data protection or security we can improve upon.

## **DATA RETENTION**

We will only keep data for as long as is required to fulfill our legal obligations. We will not keep data longer than necessary and will keep this under review.

## **DEALING WITH DATA BREACHES**

The Design Office has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of Data occur (whether in respect of you or someone else) then we will take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we will also notify the Information Commissioner's Office within 72 hours. If relevant, Data Subjects will be advised of any high risk breach.

If you are aware of a data breach you should contact our Data Protection Officer immediately and keep any evidence you have in relation to the breach.

## **SUBJECT ACCESS REQUESTS**

Data Subjects can make a 'Subject Access Request' ('SAR') to obtain a copy of the information we hold about them. This request must be made in writing.

If you would like to make a SAR in relation to your own Data, you should make this in writing to our Data Protection Officer. We will respond within one month unless the request is complex or numerous, in which case the period in which we will respond could be extended by a further two months.

There is no fee for making a SAR. However, if a request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to the request.

## **YOUR DATA SUBJECT RIGHTS**

You have the right to information about the Data we hold and process and on what basis it is held.

A Data Subject has the right to access any Data by way of a Subject Access Request (see above).

Inaccuracies in data can be corrected by contacting the Data Protection Officer.

A Data Subject has the right to request that we erase Data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected by contacting the Data Protection Officer.

A Data Subject has the right to object to data processing where we are relying on a legitimate interest, direct marketing to do so and the data subject believes that his/her rights and interests outweigh our own and you wish us to stop.

Where professionally required and legally possible, The Design Office will port your data to another Data Controller without fees.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your Data for a specific purpose, you have the right not to consent, or to withdraw your consent later, subject to contract.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website ([www.ico.org.uk](http://www.ico.org.uk)). This website has further information on your rights and our obligations.

## IMPLEMENTATION OF POLICY

This Policy takes effect from 25 May 2018 and is not retroactive.

The Design Office's Data Protection Officer is responsible for reviewing this policy and updating The Design Office's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy by email in the first instance to;

[dpo@thedesignoffice.co.uk](mailto:dpo@thedesignoffice.co.uk)

## ■ THE DESIGN OFFICE

ENDS

### **Data Protection Policy**

v2 - updated Sept 2019

The Design Office  
Chantry Mills  
6 High St  
Haverhill  
Suffolk CB9 8AZ

A copy of this document can be accessed at <https://www.thedesignoffice.co.uk/legal.php>