

Centrum Solutions

DATA PRIVACY POLICY

CONTENTS

CLAUSE

1.	Policy statement.....	1
2.	Status of the policy	1
3.	Definition of data protection terms.....	1
4.	Data protection principles	2
5.	Fair and lawful processing	2
6.	Processing for limited purposes	3
7.	Adequate, relevant and non-excessive processing	3
8.	Accurate data	3
9.	Timely processing.....	3
10.	Processing in line with data subject's rights	3
11.	Data security	4
12.	Dealing with subject access requests	4
13.	Providing information over the telephone	4
14.	Monitoring and review of the policy.....	5

1. POLICY STATEMENT

- 1.1 Everyone has rights regarding how their personal information is collected, processed and stored. During the course of our activities at Centrum Solutions we will collect, store and process personal information about our team and our clients. We recognise the need to treat it in an appropriate and lawful manner.
- 1.2 The types of information that we may be required to handle include details of current, past and prospective licensees, suppliers, clients, and others that we communicate with. The information, which may be held on paper, on a computer or in our company Customer Relationship Manager, is subject to compliance of the Data Protection Act 2018.
- 1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action.

2. STATUS OF THE POLICY

- 2.1 This policy has been approved by Centrum's company directors. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.
- 2.2 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by Leon Lloyd & Mitchell Read, Managing Directors. Any questions or concerns about the operation of this policy should be referred in the first instance to the Data Protection Compliance Manager.
- 2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Data Protection Compliance Manager.

3. DEFINITION OF 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 include 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 data.
- 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 (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

- 3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the way, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.
- 3.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our privacy policy at all times.
- 3.6 **Data processors** include any person who processes personal data on behalf of a data controller, which could include suppliers which handle personal data on our behalf. The nominated data processor is 360 Enterprise: Business & Marketing Ltd.
- 3.7 **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 with the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- 3.8 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the six enforceable data protection principles. These provide that personal data must be:

- a. used fairly, lawfully and transparently
- b. used for specified, explicit purposes
- c. used in a way that is adequate, relevant and limited to only what is necessary
- d. accurate and, where necessary, kept up to date
- e. kept for no longer than is necessary
- f. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

5. FAIR, LAWFUL AND TRANSPARENT PROCESSING

- 5.1 The Act is intended not 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 data subject must be told who the data controller is in this case Centrum Solutions,

who the data controller's representative is in this case the Data Protection Compliance Manager, the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

- 5.2 For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. The data subject's explicit consent to the processing of such data will be required.

6. PROCESSING FOR LIMITED PURPOSES

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed, and consent given before any processing occurs.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

8. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required. Data no longer being processed will be deleted every 3 years.

Processing in line with data subject's rights.

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- (a) Request access to any data held about them by a data controller.
- (b) Prevent the processing of their data for direct-marketing purposes.
- (c) Ask to have inaccurate data amended.

- (d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

10. DATA SECURITY

10.1 We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

10.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies.

10.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- (a) **Confidentiality** means that only people who are authorised to use the data can access it.
- (b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- (c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

10.4 Security procedures include:

- (a) **Password Protection.** Will be used on all digital platforms.
- (b) **Methods of disposal.** Paper documents will always be shredded.
- (c) **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

11. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them must be made in writing to the Data Protection Compliance Manager.

12. PROVIDING INFORMATION OVER THE TELEPHONE

We will never provide personal data about our licensees or clients over the telephone.

13. MONITORING AND REVIEW OF THE POLICY

13.1 This policy is reviewed annually by our board of directors in consultation with the appropriate consultative body. Recommendations for any amendments are reported to the board.

13.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.