1. Policy statement

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our employees, contractors, clients, prospective clients, newsletter recipients and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in our organisation and the services we provide.

2. About this policy

2.1 The types of personal data that Lemon Signs Limited (We) may be required to handle include names, physical addresses, email address, telephone numbers and financial information relating to our employees, contractors, clients, prospective clients, newsletter recipients and other third parties. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) (unless and until the GDPR is not applicable in the UK), each as amended and/or updated from time to time, and other regulations (Data Protection Legislation).

2.2 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, or that is provided to us by data subjects or other sources. 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.

2.3 The Data Protection Compliance Manager is responsible for ensuring compliance with the Data Protection Legislation and with this policy. That post is held by Marcin Lemiesz; 01332 987 617; info@lemonsigns.com. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

3. Definition of data protection terms

3.1 Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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

3.3 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 or an EEA national or resident. All data subjects have legal rights in relation to their personal information.

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 Data Protection Legislation.

3.5 Data users are those of our employees and contractors whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 Data processors include any person or organisation that is not a data user that processes personal data on behalf of a data controller or on its instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on the data controller's behalf.

3.7 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.

3.8 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.

3.9 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.

3.10 Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

3.11 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, including a condition requiring the express permission of the person concerned.

4. Data protection principles

Anyone processing personal data must comply with the enforceable principles of good practice. These provide that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

(b) Processed for specified, explicit and legitimate purposes and not further processed in a manner that is in compatible with those processes ('purpose limitation').

(c) Adequate, relevant and limited to what is necessary in relation to the purpose for which the data is processed ('data minimisation').

(d) 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 purpose for which it was processed is erased or rectified without delay) ('accuracy').

(e) Kept in a form which permits the identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed ('storage limitation').

(f) 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 and organisational measures ('integrity and confidentiality').

(g) Processed in line with data subjects' rights.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. Lawfulness, fairness and transparency

5.1 The Data Protection Legislation 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.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. Purpose limitation

6.1 In the course of our business (including the provision of services involving data processing to our clients), we may collect and process the personal data set out in the Schedule. This may include data we receive directly from a data subject (for example, by completing a form on a website) and data we receive from other sources (for example, where prospective clients are referred to us by existing clients).

6.2 We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the Data Protection Legislation.

7. Data minimisation

Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject by the data controller.

8. Accuracy

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

9. Storage limitation

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10. Integrity and confidentiality

10.1 Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the Data Protection Legislation and to protect the rights of data subjects

10.2 In order to ensure data protection by design and by default, we will:

(a) take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

(b) 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 will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

(c) maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(i) Confidentiality means that only people who are authorised to use the data can access it.

(ii) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(iii) Availability means that authorised users should be able to access the data if they need it for authorised purposes.

(d) Ensure that all personal data is processed within our secured and managed hosting services. Unless otherwise agreed with the data subjects in writing in advance, all data processing takes place within the EEA and all personal data remains within the EEA.

10.3 In particular, the following technical and organizational measures and processes are in place:

(a) intrusion detections and prevention measures and processes;

(b) malware protection measures and process;

(c) appropriate firewall controls and port/IP blocking;

(d) backup provision;

(e) pseudonymisation and/or encryption of data (where possible); and

(f) company mobile phones, tablets and other devices, as well as personal mobile phones, tablets and other devices, used for the purposes of accessing business emails are secured with a password and can be remotely cleared of all data in the event that any device is lost or stolen.

11.1 We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller or a data processor (right to make a subject access request).

(b) Request that any in accurate data held about them by a data controller or a data processor be amended (right to request rectification).

(c) Request that any data held about them by a data controller or a data processor be deleted in certain circumstances (right to be forgotten).

(d) Request that processing of any data held about them by a data controller or a data processor be restricted in certain circumstances (right to request restriction of processing).

(e) Request that any data held about them by a data controller or a data processor be transferred to another data controller (right to data portability).

(f) Object to the processing of any data about them by a data controller or a data processor where such processing is based solely on automated processing (including profiling) (right to object to automated individual decision-making, including profiling).

(g) Object to the processing of any data about them by a data controller or a data processor where such processing is for the purpose of direct marketing (right to object to direct marketing).

11.2 Where processing is based on consent:

(a) The controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.

(b) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of the Data Protection Legislation will not be binding.

(c) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving conse, the data subject shall be informed accordingly. It shall be as easy to withdraw as to give consent.

(d) When assessing whether consent is freely given, the data controller shall take account of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

(e) Where processing person data relating to a child on the basis of consent, the processing of that personal data shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child (and the data controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology).

12 Transferring personal data to a country outside the EEA

12.1 Personal data may be transferred outside the European Economic Area (EEA), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

12.2 We will only transfer personal data outside the EEA where one of the conditions set out in clause 12.1 has been complied with.

13. Notifying data subjects

13.1 Where personal data is collected directly from data subjects, the data controller shall inform them about:

(a) the identity and contact details of the data controller and where appropriate the data controller's data protection representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data is intended as well as the legal basis for processing (e.g. the consent of the data subject or the legitimate interests pursued by the data controller or a third party);

(d) the legitimate interests pursued by the data controller or a third party, where processing is carried out on that basis;

(e) the recipients or categories of recipients of the personal data, if any;

(f) the fact that the data controller or the data processor intents to transfer the data outside the EEA and the basis for that transfer, where applicable;

(g) the period for which the personal data will be stored or if that is not possible the criteria used to determine that period;

(h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(i) the existence of the right to withdraw consent to the processing of personal data relating to the data subject (without affecting the lawfulness of processing based on consent before its withdrawal), where processing is carried out on the basis of consent;

(j) the right to lodge a complaint with a supervisory authority (including the Information Commissioner's Office);

(k) 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 the failure to provide such data;

(l) the existence of any automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

13.2 If we receive personal data directly from the data subject, clause 13.1 shall not apply where and insofar as we can demonstrate that the data subject already has the information.

13.3 If we receive personal data from other sources (e.g. from our clients), clause 13.1 shall not apply where and insofar as we can demonstrate that the data subject already has the information, where the provision of such information proves impossible or would involve a disproportionate effort or in accordance with any other exception to this obligation expressly provided for in the Data Protection Legislation.

13.4 Where we are a data processor, we will notify the data controller without undue delay after becoming aware of a personal data breach.

14. Disclosure and sharing of personal information

14.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries.

14.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

14.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others.

This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.4 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule.

15. Dealing with requests by the data subject

15.1 Data subjects may make a request regarding any of the rights set out in clause 11.

15.2 All such requests should be made in writing and sent to the Data Protection Compliance Manager as specified in clause 2.5 (our employees will refer a request to their line manager or the Data Protection Compliance Manager for assistance in difficult situations).

15.3 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

16. Changes to this policy

This policy may change from time to time. Where appropriate, we will notify data subjects of those changes by mail or email.