Opentree Ltd

Data Protection Policy

Version 2

24th May 2018

Smart solutions.
Real support.

Contents

Clause

1. Your rights and responsibilities

1.1. Everyone has rights concerning the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our employees, customers, contract workers, consultants and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2. You, our "Data Users", are each responsible for ensuring that our business complies with this policy when you collect, store or handle personal data on our behalf. Therefore please read this policy carefully and if you have any queries about the contents please ask the Data Protection Compliance Officer, currently Andrew Frank. Breach of this policy may result in disciplinary action.

2. About this policy

2.1. The types of personal data that we may be required to handle include information about current, past and prospective employees, suppliers, clients and users of our services. We must use and store personal data, in compliance with the legal safeguards specified in the General Data Protection Regulation ("GDPR") and other legislation relating to the protection of personal data.

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.

2.3. This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4. 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.

2.5. The Data Protection Compliance Manager is responsible for ensuring compliance with the GDPR and with this policy. That post is held by Andrew Frank, who you can reach by telephone on 01642 714471 or by email at info@opentree.co.uk. Any questions about the operation of this policy or any concerns that the policy has not been followed or any recommendations you have 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, in relation to processing Personal Data, a specific, informed and unambiguous indication of the Data Subject's wishes by which s/he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Consent of the Data Subject means, in relation to processing Special Category Personal Data, where the Data Subject has given explicit consent to the processing of those personal data for one or more specified purposes and the processing is necessary (as specified in article 9(2)(a) to (j) of the GDPR).

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

3.3. **Data Subjects** means an identified or identifiable natural living person.

3.4. **Personal Data** means data relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession or that we might be able to access readily). For example, a name, address or date of birth.

3.5. **Data Controllers** are the people who, or organisations which, alone or jointly with others determine the purposes and means for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data used in our business for our own commercial purposes. We are also the Data Controller in respect of the Personal Data provided by users of our own services. Our clients are the Data Controllers of the services that we deliver on their behalf to their users where we deal with Personal Data on their behalf and as directed by them (see the definition of “Data Processors” below).

3.6. **Data Users** are those of our employees, contract workers, consultants and third party suppliers 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.

3.7. **Data Processors** include any person or organisation which processes Personal Data on behalf of the Data Controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle Personal Data on our behalf, such as a bookkeeper who handles our payroll. Where we are providing services to a client, we are the Data Processor and are responsible to that client, who is the Data Controller, for how we deal with the Personal Data generated by their customers and users during the delivery of those services.

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. **Special Category Personal Data** means 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. Special Category Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned, as set out above under the definition of Consent.

4. Data protection principles

In processing Personal Data, we must comply with the following eight enforceable principles. These provide that Personal Data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with Data Subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated outside the European Economic Area in countries without adequate protection.

5. Fair and lawful processing

5.1. The GDPR 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, we must process it on the basis of one of the legal grounds set out in the GDPR which include:

(a) The Data Subject has consented to the processing.

(b) The processing is necessary for the performance of a contract with the Data Subject.

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

(d) The processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed.

(e) The processing is necessary to protect the vital interests of the Data Subject.

5.3. When Special Category Personal Data is being processed, we must meet other additional conditions. The most common of these is that any consent given must be explicit and cannot be implied from the Data Subject's actions.

5.4. It's quite possible for us to find ourselves processing Special Category Personal Data unexpectedly when providing our document management service. We will remain alert to these issues and their implications at all times.

5.5. When processing Personal Data as data controllers in the course of our business, we will ensure that those requirements are met. When we process Personal Data on behalf of others, we are responsible to them for ensuring that those requirements are met.

5.6 When we process Personal Data mostly our lawful basis will be contractual. In some circumstances we will process personal data because we have legal obligations to do so. For example keeping records of HMRC purposes or information about the health of our employees. In other cases we will have a legitimate business interest to process personal data. In this scenario we have to record the fact that we have considered (i) the legitimacy of such interest and (ii) the rights and freedoms of the data subjects whose data we wish to process and assessed that their rights and freedoms are not damaged by our proposed use.

6. Processing for limited purposes

6.1. In the course of our business, we may collect and process the Personal Data (for example name, address, email address and telephone number). This may include data we receive directly from a Data Subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2. We will only process Personal Data for the purpose of delivering our services to the user or for any other purposes specifically permitted by the GDPR. We will notify those purposes

to the Data Subject when we first collect the data or as soon as possible thereafter. Where such processing is further to an agreement to supply services the purpose is usually set out in the agreement.

7. Notifying Data Subjects

7.1. If we collect Personal Data directly from Data Subjects, we must inform them about:

(a) The purpose or purposes for which we intend to process that Personal Data.

(b) The types of third parties, if any, with whom we will share or to which we will disclose that Personal Data.

(c) The means, if any, with which Data Subjects can limit our use and disclosure of their Personal Data.

We do this by referencing our Privacy Policy which can be found at https://www.opentree.co.uk/wp-content/uploads/2018/05/Opentree-Privacy-Policy.pdf

If we receive Personal Data about a Data Subject from a third party, the third party confirms that either:

(d) The Data Subject has a contractual relationship with the third party and knows that the third party will be transferring the Data Subject's data to us for specific purposes.

(e) S/he has appointed the third party to act on his/her behalf and has agreed that the third party can:

i. Give consent on his/her behalf to the processing of his/her personal data

ii. Receive on his/her behalf any data protection notices.

7.2. If applicable, we will also inform Data Subjects whose Personal Data we process that we are the Data Controller with regard to that data, and who our Data Protection Compliance Manager is. For Data Subjects whose Personal Data we are processing as a Data Processor on behalf of a client or other third party (the Data Controller), we will refer any enquiry they may have relating to their Personal Data to the Data Controller and will intervene only in the event that the Data Controller fails for some reason to comply with its legal obligations.

8. Adequate, relevant and non-excessive processing

We will only collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject. If you believe that we are processing certain Personal Data unnecessarily please inform the Data Protection Compliance Officer.

9. Accurate data

Where we act as a Data Controller we will do our best to 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. Where we act as a Data Processor we will require the Data Controller to meet these obligations.

10. Timely processing

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. Our proposed retention periods are set out in our Privacy Policy.

11. Processing in line with Data Subject's rights

11.1 We will process all Personal Data in line with Data Subjects' rights, in particular their right to:

(a) Be informed.

(b) Request access to any data held about them by a data controller (bearing in mind that this may or may not be us).

(c) Prevent the processing of their data for direct-marketing purposes.

(d) Ask to have inaccurate data amended.

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

(f) Ask to have their data erased.

11.2 If you receive a request from a Data Subject in relation to exercising their rights please forward this to the Data Protection Compliance Officer. Our Privacy Policy sets out what is required from a Data Subject and see further information at section 15 below.

12. Data security

12.1. We will process all Personal Data we hold in accordance with our security policies and will, at all times, take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data, as set out below and as further advised from time to time.

12.2. We will 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, and where there is an agreement in place confirming this.

12.3. We will maintain data security by protecting 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 the our central systems instead of individual devices.

12.4. Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed or securely erased when they are no longer required.

(d) **Equipment.** Data users must ensure that their displays do not show confidential information to passers-by and that they log off from their devices left unattended. Everyone should ensure that they're using secure passwords at all times or such other secure access functionality as we may use from time to time (such as fingerprint scanners). If you think somebody else, whoever that might be, may know what your password is, it is your responsibility to change it immediately.

13. Data Protection Breach

13.1. If a potential or actual breach is anticipated or identified, you shall immediately notify the Data Protection Compliance Manager (as we may have an obligation to inform the Information Commissioners Office ("ICO") within 72 hours) and provide sufficient information for the Manager to assess the severity of the breach and who might be affected and what further steps are required.

13.2 A Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or processed. The following are examples of data breaches:

(a) access by an unauthorised third party;

(b) deliberate or accidental action (or inaction) by a data controller or data processor;

(c) sending Personal Data to an incorrect recipient;

(d) computing devices containing Personal Data being lost or stolen;

(e) alternation of Personal Data without permission;

(f) loss of availability of Personal Data.

13.3 **For the avoidance of doubt being involved in a data breach is not a disciplinary matter. However not promptly reporting a breach or potential breach is a disciplinary matter**.

13. Transferring Personal Data to a country outside the EEA

13.1. We may transfer any Personal Data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies and we have a record of this:

(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 GDPR, 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.

13.2. Subject to meeting the requirements in clause 13.1 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff maybe engaged in, among other things, the fulfilment of contracts with the Data Subject, the processing of payment details and the provision of support services.

14. Disclosure and sharing of personal information

14.1. 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.

14.2. 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.

15. Dealing with subject access requests

15.1. Data Subjects must make a formal request for information we hold about them. This must be made in writing (which includes an email or some other electronic message that can be permanently recorded and is not transient in nature). Employees who receive a written request should forward it to the Data Protection Compliance Manager immediately. We will deal with all such requests promptly and sensitively.

15.2. 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.

15.3. From time to time, it is possible that we may make mistakes. The important thing is that when this happens, we can demonstrate the reasoning behind the decisions we have made and that we have taken action to correct the mistake as quickly as possible.

16. Changes to this policy

This policy will be updated from time to time - check the version numbers and date at the top if you're not sure whether you're using the correct version.