DATA PRIVACY POLICY
Relating to GDPR

May 2018

AVOCET

Table of Contents

1. Policy statement

1.1. Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information for our own administrative purposes (including employee administration and sales) and on behalf of our customers. We recognise the need to treat all information 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 employees, suppliers and our customers and for our own administrative purposes as a data controller. We also undertake processing as a data processor on behalf of our customers in the course of providing our services to them. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and other regulations. GDPR imposes restrictions on how we (and our customers) may use that information.

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 by employees will be taken seriously and may result in disciplinary action including dismissal and prosecution.

2. Status of the policy

2.1. This policy 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 in our capacity as both a data controller and data processor.

2.2. Any questions or concerns about the operation of this policy should be referred in the first instance to the Directors.

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 Directors or the Data Protection Officer.

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 either for our own purposes or as a data processor on behalf of our customers. 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 manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with GDPR. We are the data controller for all processing that we do for our own administrative purposes (including employee and supplier management) but not for the processing that we do on behalf of customers.

3.5. "Data users" include our employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6. "Data processors" include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf. We act as a data processor when we process personal data on behalf of our customers in the course of providing the services ("our services") to them.

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 on 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

4.1. Anyone processing personal data must comply with the eight enforceable principles of good practice. 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 in countries without adequate protection.

5. Fair and lawful processing

6. GDPR 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 when processing data (for our own administrative purposes, this is {*Company Name*}), 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. Customers or partners should provide this information to data subjects when they act as data controllers and we process personal data on their behalf as a result of providing access and use of our services.

6.1. For personal data to be processed lawfully, the data controller must ensure that certain conditions have been 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. In most cases the data subject's explicit consent to the processing of such data will be required.

7. Processing for limited purposes

7.1. 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 GDPR. 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 of the new purpose before any processing occurs. This responsibility lies with other controllers when we process personal data on their behalf.

8. Adequate, relevant and non-excessive processing

8.1. 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. This responsibility also lies with schools when we process personal data on their behalf.

9. Accurate data

9.1. Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should 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 should be destroyed. We expect other data controllers to ensure that any data that we process on their behalf is accurate and up to date.

10. Timely processing

10.1. 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. We also expect other controllers and processors to ensure that personal data is not kept for longer than is necessary.

11. Processing in line with data subject's rights

11.1. Data must be processed in line with data subjects' rights.

Data subjects have a right to:

a) Be informed about the collection and use of their data.
b) Request access to any data held about them by a data controller.
c) Request to restrict or supress the use of their personal data.
d) Ask to have inaccurate data amended.
e) Have their personal data erased 'the right to be forgotten'
f) Data portability to obtain and reuse their data for personal use across multiple services.
g) Object to processing based on legitimate interests, profiling and direct marketing or scientific , historical or statistical use.
h) Information regarding any automated decision making and profiling.

11.2. We may, from time to time, need to provide other controllers or processors with assistance to enable them to respond to any such assertion of these rights by data subjects.

12. Data security

12.1. 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.

12.2. When we act as a data controller (in respect of the personal data we hold for our own administrative purposes), GDPR 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, or if they put in place adequate measures themselves. When we process personal data on behalf of other controllers, our obligations concerning data security are imposed through our contract with the data controller.

12.3. 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 a central computer system (cloud or on premise) instead of individual PCs.

13. Security procedures include:

13.1. "Entry controls." Any stranger seen in entry-controlled areas should be reported.

13.2. "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.)

13.3. "Methods of disposal." Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

13.4. "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.

14. Dealing with subject access requests

14.1. A formal request from a data subject for information that we hold about them (either for our own purposes, or on behalf of another controller or processor) must be made in writing, email or via our online form. A fee may be payable by the data subject for provision of this information where unreasonable cost is incurred in processing the

request. Any member of staff who receives a written request should forward it to their manager immediately.

15. Providing information over the telephone

15.1. Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular, they should:

a. Check the caller's identity to make sure that information is only given to a person who is entitled to it.
b. Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked. When the request relates to personal data that we process on behalf of another controller or processor, the caller should direct their request to the relevant party.
c. Refer to their manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

16. Monitoring and review of the policy

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

If you have any questions about this policy, please contact:

Norman Taylor
Director
Data Lead

Avocet Consult Limited
Aldo House,
Kempson Way,
Bury St Edmunds,
Suffolk,
IP32 7AR