Data Protection and Security Policy

Sep 2017

Contents

1.	Introduction		3
2.	Definitions		3
3.	Data Protection Principles		4
	3 .1	Principle 1 - Fair & Lawful Processing	5
	3 .2	Principle 2 - Collection & Processing for Specified & Lawful Purposes	7
	3 .3	Principle 3 - Adequate, Relevant and Not Excessive	7
	3 .4	Principle 4 - Accurate & Up to Date	7
	3 .5	Principle 5 - Kept For No Longer Than Is Necessary	8
	3 .6	Principle 6 - Processed in Accordance With The Rights Of Data Subjects	8
	3 .7	Principle 7 - Security and Technical and Organisational Measures	9
	3 .8	Principle 8 - Overseas Transfers	9
4.	Confidential Information		10
5.	Contacts		10

1. Introduction

vCreate is committed to preserving the confidentiality and integrity of all information it holds and processes and to operating its business in compliance with the requirements of the UK Data Protection Act 1998, the EU Data Protection Directive (95/46/EC) and related rules.

We recognise the importance of Personal Data and of respecting the privacy rights of individuals. This Data Protection & Security Policy ("Policy") sets out the principles which we apply to our Processing of Personal Data and use of Confidential Information so that we not only safeguard one of our most valuable assets, but also that which belongs to our customers and employees. For the most part we process this information in one of two capacities, either: (i) as a Data Controller for our own internal business operations, such as human resources, administration, marketing, sales etc. or (ii) as a Data Processor when carrying out our software-as-a-service (or "SaaS") operations for our customers.

Although the Legislation places most of the obligations upon the Data Controller, it is the responsibility of all vCreate employees to apply the provisions of this Policy in relation to all Processing of Personal Data and handling of Confidential Information, whether vCreate is acting as Data Controller or Data Processor (or both). vCreate provides employees with regular instruction in respect of such matters.

Any questions about this Policy should be raised with vCreate directly, details are at the end of this Policy.

2. Definitions

The following key words and phrases are used within this Policy:

"Confidential Information"
means all information (however recorded, preserved or disclosed) disclosed to vCreate or its representatives, whether or not marked as "confidential", including but not limited to:

Personal Data, any information designated as confidential or commercially sensitive or that which is, by its nature, clearly confidential, the business, affairs, customers, clients, suppliers, plans, developments, intentions, or market opportunities of the disclosing party or of the disclosing party's group;
the operations, processes, product information, know-how, designs, trade secrets or software of the disclosing party or of the disclosing party's group; and any information or analysis derived from Confidential Information;

but not including any information that:

is or becomes generally available to the public other than as a result of its disclosure by vCreate in breach of this Policy; was available to vCreate on a non-confidential basis prior to disclosure by the disclosing party; is received by vCreate from a third party who lawfully acquired or developed it and who is under no obligation of confidentiality in relation to its disclosure; the parties agree in writing is not confidential or may be disclosed; or is independently developed by vCreate without the use of the disclosing party's Confidential Information.

"Data"
means information that is processed electronically (e.g. by computer); is recorded manually (e.g. on paper) with the intention of being processed electronically; or is recorded as part of any filing system structured by reference to individuals or criteria relating to them in such a way that specific information relating to a particular individual is readily accessible;

"Data Controller"
means the organisation that determines the purposes for which and the manner in which Personal Data are processed;

"Data Processor"
means the organisation that processes Personal Data on behalf of the Data Controller;

"Data Subject"
means a living, identifiable individual about whom Personal Data is processed;

"Personal Data"
means Data which relate to a living individual who can be identified from those Data or from those Data and other information which is in the possession of or is likely to come into our possession as Data Controller or Data Processor, as the case may be. Personal Data include opinions and any indications of our intentions towards an individual;

"Processing"
includes obtaining, recording, holding, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying Personal Data;

"Sensitive Personal Data"
means information about the Data Subject relating to the (a) racial or ethnic origin, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) trade union membership, (e) physical or mental health or condition, (f) sexual life, (g) commission or alleged commission by any offence, and (h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

3. Data Protection Principles

vCreate is committed to complying with the data protection principles set out in the Legislation. Under the UK Data Protection Act, these are set out as eight data protection principles, under which Personal Data must:

- be processed fairly and lawfully;
- be obtained and processed only for one or more specified and lawful purposes;
- be adequate, relevant and not excessive in relation to the purpose;
- be accurate and, where necessary, kept up to date;
- be kept for no longer than is necessary for the purpose;
- be processed in accordance with the rights of Data Subjects under the Legislation;
- be held securely and appropriate technical and organisational measures must be taken against unauthorised or unlawful Processing and against accidental loss, destruction or damage;
- not be transferred to a country or territory outside the European Economic Area unless adequate protection is in place.

Further details of how vCreate complies with these principles are set out below.

3.1 Principle 1 - Fair & Lawful Processing

Fair Processing

The Legislation requires that Personal Data must be processed fairly. This means the Data Controller must ensure transparency of Processing so that Data Subjects are aware of who is Processing their Personal Data and why. This is primarily an obligation on the Data Controller who determines what is being processed and is much less relevant to a Data Processor who does not determine what is processed. This obligation affects vCreate primarily when acting as a Data Controller in relation to the operation of our own internal business.

In the case of vCreate marketing activities e.g. advertisement of vCreate products and services on our website, we include a description of the communication channels that we intend to use. If any of those channels involve marketing by email, SMS, fax or automated calling systems, we will (as a general rule) obtain the Data Subject's consent by means of a suitable (reversible) opt in provision. Where we obtain Personal Data directly from the Data Subject (e.g. as a result of a telephone call, or online capture) we give the notice to the Data Subject at the time we obtain their Data. Where we obtain Personal Data about a Data Subject from a third-party source (e.g. an agent) we provide the data protection notice as soon as reasonably practicable after we have started Processing their Data (unless it would be a disproportionate effort to do so).

Accordingly where we act as a Data Processor for our SaaS customers, the obligation to issue any necessary data protection notices rests with our customer.

Lawful Processing

This is primarily an obligation for Data Controllers and for the most part only affects vCreate in the operation of our own internal business. vCreate will only process Personal Data where it is justified under one of the following conditions:

the Data Subject has given his consent to the Processing; or the Processing is necessary:

- in order to enter into or perform a contract with the Data Subject;
- for compliance with a legal obligation to that applies to vCreate (other than an obligation under a contract);
- in order to protect the vital interests of the Data Subject (i.e. a life or death situation);
- for the purposes of legitimate interests pursued by the Data Controller or by the third party to whom the information is disclosed, except where the Processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject.

Processing Sensitive Personal Data

In addition, where vCreate processes Sensitive Personal Data, due to the sensitive and sometimes confidential nature of this category of Personal Data we will only process Sensitive Personal Data where it is justified under one of the following additional conditions:

- the Data Subject has given explicit consent to the Processing; or
- the Processing is necessary for:
    - vCreate to comply with employment law;
    - the protection of the vital interests of the Data Subject or another person, where the Data Subject's consent cannot be given or has been unreasonably withheld, or where the Data Controller cannot reasonably be expected to obtain consent;
    - the purposes of legal proceedings or for obtaining legal advice, or otherwise for establishing, exercising or defending legal rights;
    - medical purposes and is undertaken by a health professional or someone subject to an equivalent duty of confidentiality;
    - monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of Data Subjects
    - the prevention or detection of any unlawful act, and must necessarily be carried out without the explicit consent of the Data Subject being sought so as not to prejudice those purposes;
    - research purposes in the substantial public interest and it does not support measures or decisions with respect to any particular Data Subject and does not cause, nor is likely to cause, substantial damage or distress to the Data Subject or any other person.

3.2 Principle 2 - Collection & Processing For Specified & Lawful Purposes

The Legislation requires that Personal Data must be obtained by Data Controllers only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

Accordingly the purposes for which vCreate will process Personal Data as a Data Controller are set out below:

- Staff Administration
- Advertising, Marketing and Public Relations
- Advertising, Marketing and Public Relations on behalf of customers
- Accounts and Records
- Consultancy and Advisory Services
- Information and databank administration.

vCreate will not process Personal Data for any other purpose unless the Data Subject gives consent. Where vCreate acts as a Data Processor for a SaaS customer the responsibility for obtaining any such consent rests with the relevant SaaS customer.

3.3 Principle 3 - Adequate, Relevant And Not Excessive

The Legislation requires that Personal Data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed and that it must be kept up to date.

To fulfil the requirement for Personal Data to be adequate, relevant and not excessive, vCreate ensures that when acting as Data Controller:

- we identify the Personal Data needed for a particular purpose and we collect the minimum amount required to properly fulfil that purpose;
- we do not hold Personal Data on a 'just-in-case' basis or because we think it might be useful in the future except where a Data Subject consents, e.g. a prospective employee agrees to us retaining Personal Data should a suitable vacancy arise;
- we keep Data up to date; and
- we do not keep Data for too long.

3.4 Principle 4 - Accurate & Up To Date

When inputting Data onto our system in our capacity as a Data Controller, vCreate takes reasonable steps to ensure the Data is accurate and may contact Data Subjects for clarification if we are unsure as to the accuracy of certain information.

vCreate will not be in breach of this principle, even if we are holding inaccurate Data if:

- we accurately recorded those Data when we received them from the Data Subject or a third party;
- we took reasonable steps to ensure the accuracy of those Data; and
- if the Data Subject has notified us that the Data are inaccurate, we have taken steps to indicate this fact.

vCreate takes reasonable steps to keep Data up to date to the extent necessary.

3.5 Principle 5 - Kept For No Longer Than Is Necessary

The Legislation requires that Personal Data processed for any purpose must not be kept for longer than is necessary for that purpose.

vCreate reviews the Personal Data it holds on a regular basis and, where relevant, securely removes any Data which is no longer required in connection with the purpose for which it was originally obtained. Securely removes means that any printed material is appropriately shredded or electronic media has the record removed from it relating to the subject including from backups, in a manner that the material is not normally retrievable.

Where vCreate acts as Data Processor and holds Data on its servers on behalf of its customers that the customer has input directly into vCreate's system, the customer will be responsible for maintaining such Data and deleting any Data that is no longer required. vCreate will return or destroy all Data held on behalf of a SaaS customer in accordance with the terms of the relevant contract with that customer.

3.6 Principle 6 - Processed In Accordance With The Rights Of Data Subjects

Data Subjects have certain rights under the Legislation to access their Data and to prevent processing in certain circumstances. Most requests will come from our employees where vCreate is a Data Controller, although vCreate will also have to respond to subject access requests from the customers of our SaaS customers.

Right of Subject Access

If vCreate receives a written request from a Data Subject for access to his/her Personal Data, we will respond within 40 days of receipt of the request and provide a description of:

- the Personal Data relating to that Data Subject;
- the purposes for which the Data are being processed;
- the recipients of the Data;
- the information constituting the Personal Data; and
- the source of those Data (if available).

vCreate reserves the right to charge the Data Subject a fee for the provision of this information as defined by the Legislation. Where the Data is held on behalf of a SaaS customer, vCreate will notify that customer of such request for access and give the SaaS customer the option to deal with the request itself.

Right to Prevent Processing Likely to Cause Damage or Distress

Data Subjects have the right to ask us not to process their Personal Data if the Processing of the Data in a particular way or for a particular purpose is causing, or is likely to cause, damage or distress to that Data Subject or another person; and that damage or distress is, or would be, unwarranted.

If we receive a written request from any person exercising this right, we will respond within 21 days of receipt of the request and confirm that we have either complied or intend to comply with the request, or stating our reasons for non-compliance. Where this occurs in the case of vCreate acting as a Data Processor for a SaaS customer, the request must be forwarded to the relevant SaaS customer and the Data Subject advised whether vCreate has the authority to cease processing the Personal Data.

Right to Prevent Processing for the Purposes of Direct Marketing

If we receive a request from a Data Subject that we stop Processing their Personal Data for direct marketing purposes, we will take the appropriate action to ensure that the individual's details are suppressed on our marketing database and the individual is no longer contacted by us for marketing purposes.

Right to Object to Automated Decision Taking

Data Subjects have the right to object to automated decisions being taken about them in relation to important matters that significantly affect them (such as evaluating performance at work, creditworthiness, reliability or conduct).

If we receive a written request from any person exercising this right, we will respond within 21 days of receipt of the request and inform the individual of the steps that we intend to take to comply with the request. Where this affects the services being provided to a SaaS customer, vCreate will notify the relevant SaaS customer before responding to the Data Subject.

3.7 Principle 7 - Security And Technical And Organisational Measures

The Legislation requires vCreate to take appropriate technical and organisational measures to safeguard Personal Data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

vCreate has put in place a number of technical and organisational measures and procedures which we apply not only to Personal Data, but also to all information we hold, including Confidential Information and information of any other kind that is used within the business.

Details of our technical and organisational measures are available upon request.

Where vCreate uses third parties to process Personal Data on our behalf, they will be acting as our Data Processors and we will ensure that we:

- put in place a contract in writing with each of our Data Processors under which they agree to act only on instructions from us;
- include the right to audit our Data Processors to ascertain compliance with the data protection requirements in their contract; and
- ensure that the Data Processor agrees to comply with obligations equivalent to those set out in this Policy.

3.8 Principle 8 - Overseas Transfers

The Legislation requires that Personal Data must not be transferred to a country or territory outside the European Economic Area (i.e. the member states of the EU plus Iceland, Liechtenstein and Norway), unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

vCreate has put in place measures and procedures to ensure that any Personal Data transferred outside the EEA is adequately protected and that local privacy laws are observed.

4. Confidential Information

vCreate will keep Confidential Information (which of course extends beyond Personal Data) it receives confidential and, except with the prior written consent of the disclosing party, and will:

- not use or exploit the Confidential Information in any way except for the purposes for which it has been disclosed;
- not disclose or make available the Confidential Information in whole or in part to any third party, except as expressly permitted by the disclosing party;
- not copy, confirm in writing or otherwise record the Confidential Information except as strictly necessary for the purposes for which it has been disclosed and any such copies, confirmations or records shall remain the property of the disclosing party

vCreate may only disclose the Confidential Information to those of our employees who need to know this Confidential Information for the purposes for which it has been disclosed, provided that:

- we inform those employees of the confidential nature of the Confidential Information before disclosure;
- at all times, we are responsible for compliance of those employees with the obligations set out in this Policy and the technical and organisational measures; and
- the employees receive the training required under the technical and organisational measures prior to such disclosure.

vCreate may disclose Confidential Information to the extent such Confidential Information is required to be disclosed by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction provided that, to the extent we are legally permitted to do so, we give the other party as much notice of this disclosure as possible.

vCreate may, provided that we have reasonable grounds to believe that the disclosing party is involved in activity that may constitute a criminal offence under the Bribery Act 2010, disclose Confidential Information to the Serious Fraud Office without first notifying the disclosing party of such disclosure.

At the request of the disclosing party, vCreate shall:

- destroy or at vCreate's discretion, return to the disclosing party all documents and materials (and any copies) containing, reflecting, incorporating, or based on the disclosing party's Confidential Information;
- erase all the disclosing party's Confidential Information from its computer systems or which is stored in electronic form (to the extent possible); and certify in writing to the disclosing party that it has complied with the requirements of this clause, provided that vCreate may retain documents and materials containing, reflecting, incorporating, or based on the Confidential Information to the extent required by law or any applicable governmental or regulatory authority and to the extent reasonable to permit vCreate to keep evidence that it has performed its obligations under any agreement with the disclosing party.

5. Contacts

If you have any queries regarding this Policy or its Schedules please email dataprotection@vcreate.tv.

6. Amendments To This Policy

This Policy and its Schedules will be updated from time to time by vCreate to reflect any changes in legislation or in our methods or practices.

Date of issue: Sep 2017