k

Crunch Payments

Data Protection Policy

Website Copy

VERSION CONTROL

The name/s below certify that this policy has been reviewed, and demonstrates that senior management are aware of all the requirements contained herein and are committed to ensuring compliance with such requirements.

Version	Date	Status	Author	Reviewer (R) Approved (A)	Released
1	01/06/18	Draft	Crunch Compliance Function	Board	01/06/18

AMENDMENT RECORD

This policy is reviewed to ensure its continuing relevance to the procedures and process that it describes. A record of additions or amendments is given below:

Page	Context	Revision	Date
Whole Text	Company restructuring and new name	Amendments made to reflect change of company name and status	24/09/19

CONTENTS

1. Policy Statement

The Data Protection Act arose following concerns that the availability and ease of manipulation of personal information within computer systems was threatening the privacy of individuals.

In UK the Data protection Act 1998 was enacted into law in the UK, transposing Directive 95/46/EC of the European Parliament and the Council of the 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This was subsequently modified by the UK Data Protection (Amendment) Act 2003 and superseded by the General Data Protection Regulation (GDPR) which came into force on the 24th May 2018. This Regulation will be transposed into the local legislation of member states of the European Union.

Crunch Payments has a duty to ensure compliance with all relevant provisions of the GDPR.

The Regulations set out the rules for the processing, keeping and distribution of personal information and apply to paper records in a *relevant filing system* and computer records. *Relevant Filing System* is one where the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that "specific information relating to a particular individual is readily accessible".

The types of personal data that Crunch may be required to handle include information about current, past and prospective suppliers, cardholders, employees and others that we communicate with. The personal data, which can be stored in a wide range of formats, is subject to legal safeguards specified in GDPR and other regulations.

The Regulations give individuals certain rights to review data held about them and to have inaccurate data corrected or deleted and a right to be forgotten whilst requiring those who record and use personal information (either manual or computer records) to be open about that use and to follow sound and proper practices.

Crunch handles information of a personal nature and as is registered with the respective Data Protection authorities in the UK, which requires putting in place policies to ensure compliance with the legislation. This Policy has been designed for this purpose. Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

Crunch is registered with the Information Commissioners Office "ICO" for the purpose of Data Protection.

2. Definition of Data Protection Terms

Controller; the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data Subject; an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Data Users; our employees, agents or representatives whose work involves processing personal data;

GDPR; Regulation (EU) 2016/679 of the European Parliament and of the Council, (the General Data Protection Regulation);

Personal Data; means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing; any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor; a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

3. Policy Scope

Data Protection Principles

Whosoever is employed by Crunch, including relevant outsourced service providers, and processes personal data must comply with the following principles as set out in the GDPR and which must form part of good information handling practice.

In accordance with the requirements of GDPR, personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
- 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 or organisational measures ('integrity and confidentiality');

Where Crunch is acting in its capacity as a Controller, it shall be responsible for ensuring that:

- Its data related activities are carried out in a manner which complies with each of the aforementioned principles; and
- It is able to demonstrate its compliance with each of the aforementioned principles;

The principles are intended to protect the rights of individuals about whom Crunch records personal data. As the principles are only expressed in general terms, detailed information handling procedures need to be implemented so as to ensure that the principles are complied with within Crunch. In order to achieve this, employees must be given suitable periodic training so that they are aware of their individual and collective responsibilities.

4. Collection and Use of Data within Crunch

All personal data must be obtained in accordance with the GDP Regulations. The person disclosing the data, "Data Subject", must be made aware of the uses to which that data will be put and must consent to those uses before the data is passed to Crunch. Data can only be used for the purposes consented to by the Data Subject.

All data must be accurate and kept up to date. Wherever possible, the Data Subject should be invited to check and confirm the accuracy of the data. This applies when data is first collected and whenever use is subsequently made of that data.

All Data Subjects have the legal right to review data held about them by Crunch. Wherever possible, only factual data should be stored. Where other data (e.g. details of telephone conversations or (meetings) has to be stored, then it must be objective and honest, and must not include personal opinions.

When discussing or revealing data over the telephone to a caller who has questions relating to the information held, checks must be made to confirm that the person making the request is in fact the Data Subject. Date of birth or some other personal detail could be used to confirm identity. If you are not sure of the person's identity, then the request for the personal data should be made in writing to Crunch.

Personal data will not be kept any longer than necessary for the purpose(s) for which it was collected. 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.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set down within GDPR. Typically, we rely upon one or more of the following grounds to justify the processing of personal data:

- The data subject providing consent to the processing of his or her personal data for one or more specific purposes;

- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

- The processing is necessary for compliance with a legal obligation to which we, in our capacity as either a Processor or Controller are subject to; and

- The processing is necessary for the purposes of legitimate interests pursued by us, in our capacity as a controller;

When processing personal data in the course of business, whether in the capacity of Processor or Controller, which will depend on the circumstances, we will ensure that processing is justified on at least one of the aforementioned grounds or on such other grounds as are provided for within GDPR.

All personal data which is received will only be processed for the specific purposes set down in our data inventories or for other purposes specifically permitted by GDPR, these inventories will be updated on a periodical basis.

All personal data will be processed in accordance with the Data Subjects rights which include:

- The right of access;

- The right to rectification;

- The right to erasure, (otherwise referred to as the 'right to be forgotten');

- The right to restriction of processing;

- The right to data portability;

- The right to object;

The right not to be subject to a decision based solely on automated processing;

5. Transferring Data Outside the EU

Under the Regulations, transfers of personal data to countries outside the EEA are prohibited unless either:

- The transfer is made on the basis of an adequacy decision of the European Commission;

- The transfer is made subject to appropriate safeguards;

- The transfer is made in accordance with binding corporate rules; or
- The transfer is made in accordance with a specific derogation set down within GDPR;

In determining what makes a destination country adequate, it is possible to either rely on a published European Commission decision, or to make an assessment of adequacy based on a number of factors such as the nature of the data being transferred and the purposes for which they are being transferred, the law in the country in question and any security measures being taken.

If the destination country outside the EEA does not have adequate data protection laws in place, then the transfer will only be permitted where one or more specified preconditions can be met, such as where the data subject has consented, the transfer is necessary for the performance of a contract with the data subject or the rights of the data subject are protected by a contract based on the European-approved terms in place between the sender and the recipient of the data.

6. Data Protection by Design and Default

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, we shall, 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, such as pseudonymisation and tokenisation for a PAN, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights of data subjects.

Furthermore, we shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

7. Contracts with Third Parties

When any sub processing of personal data is carried out by a data processor (third party) on behalf of Crunch, the following protections will apply:

- The processing will be carried out under contract, which is evidenced in writing and under which the third party is to act only on instructions from Crunch. Crunch will be directed by the Controller as to what personal data should be collect for the process where appropriate;
- The contract will also require the third party to give assurances and guarantees that they will only process the data as directed by Crunch;
- Third party must provide guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- Crunch will be able to conduct audit visits to ensure compliance with the above measures;

8. Data Security

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

We will put in place procedures and systems 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 another data processor if the processor in question operates adequate data security measures.

To guard against the accidental loss, destruction or damage to personal data, Crunch will operate a comprehensive back up and disaster recovery plan for all data recorded.

9. Subject Access

Any individual has the right to be told whether any personal data is held about him by Crunch and, if so, to be supplied with a copy of that data, the individual also has the right to have his data amended and deleted.

Where Crunch is acting as a Processor in respect of the individual's data, a Subject Access Request will need to be made to the Controller, who will review and decide if the request is justifiable. If it is the request will be passed to Crunch to deal with. In the case of Crunch acting as a Controller in respect of individual's data, Crunch will deal with this internally. In both instances it will be necessary
To follow the Data Subject Access Request Procedure that can be found at Appendix 1 of this document.

In addition, where data is processed automatically, and is likely to form the sole basis for any decision significantly affecting the data subject, then the individual will also be entitled to know the logic involved in the decision making process.

Crunch must bear in mind that any response will need to include data held on Crunch's systems within other companies of its Group. Crunch has 30 days in which to respond, and any such formal request for the release of information to an individual must be immediately reported to the company's Compliance Department.

10. Breaches of Requirements

All individuals involved in handling personal data or otherwise with responsibility for this area, have a duty to report promptly any breaches of the data protection requirements to Crunch Compliance Manager.

A report will be provided to the Board together with recommendations for remedial actions to be taken. It will be necessary to notify the Issuer or Controller of any such breaches immediately along with the relevant body where deemed necessary.

11. Compliance function responsibilities:

- register these declarations of breaches in data protection within the companies Data Breach register
- keep this record for total of five years after a member of the board or associated responsible person resigns or is removed from his position in relation to Crunch
- keep this record for all serving members of the board or other active responsible persons
- present the Board with each of the declared disclosures and the Board will decide an appropriate course of remedial action
- the Register is to be reviewed quarterly or thereabouts by the Board if no amendments have been made during this time

Disclosure, monitoring and review

Where a breach of data has been disclosed, the Board member or other responsible person concerned may not, without prior consent or the conflict declared as accepted or maintained, vote on that item or take part in any Board or Sub Committee discussion on that topic. The Chairperson and the remaining persons attending the meeting can on a case by case basis, reach unanimous agreement on an appropriate course of action.