DATA PROTECTION POLICY

Introduction

Purpose

Cannon Fire Protection Ltd (CFP) is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of Job Applicants, Employees, Contractors, Volunteers, Apprentices and former Employees, referred to as HR-related personal data. This policy does not apply to the personal data of Clients or other personal data processed for business purposes.

CFP has appointed Phil Burgin (Operations Director) as the person with responsibility for data protection compliance within the organisation. He can be contacted at phil@cannonfire.co.uk. Questions about this policy, or requests for further information, should be directed to him.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection principles

CFP processes HR-related personal data in accordance with the following data protection principles:

- CFP processes personal data lawfully, fairly and in a transparent manner
- CFP collects personal data only for specified, explicit and legitimate purposes
- CFP processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- CFP keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- CFP keeps personal data only for the period necessary for processing
- CFP adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

We will let you know the reasons for processing your personal data, how we use such data and the legal basis for processing in our Privacy Notices. We will not process personal data for other reasons. Where we rely on our legitimate interests as the basis for processing data, we will carry out an assessment to ensure those interests are not overridden by the rights and freedoms of any individuals.

Where we processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

CFP will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment, contractor or volunteer relationship or apprenticeship is held within the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its Privacy Notices.

We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As a data subject, you have a number of rights in relation to your personal data.

Subject Access Requests

You as an individual have the right to make a Subject Access Request. Should you do this, we will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from yourself
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- for how long your personal data is stored (or how that period is decided)
- your rights to rectification or erasure of data, or to restrict or object to processing
- your right to complain to the Information Commissioner if you think CFP has failed to comply with your data protection rights; and
- whether or not we carry out automated decision-making and the logic involved in any such decision-making

CFP will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if this request has been made electronically, unless you agree otherwise.

To make a Subject Access Request, you should send the request to hr@assetprotectiongroup.co.uk or use CFP's form for making a Subject Access Request, available from the HR Department. In some cases, we may need to ask for proof of identification before the request can be processed. CFP will inform you if we need to verify your identity and the documents we require.

We will normally respond to a request within a period of one month from the date it is received. In some cases, which include processing large amounts of data, we may respond within three months of the date the request is received. We will write to you within one month of receiving the original request to tell you if this is the case.

If a Subject Access Request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A Subject Access Request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If a request is submitted that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

Other rights

You have a number of other rights in relation to your personal data. They can require us to:

- rectify inaccurate data
- stop processing or erase data that is no longer necessary for the purposes of processing
- stop processing or erase data if the individual's interests override CFP's legitimate grounds for processing data (where CFP relies on legitimate interests as a reason for processing data)
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests as an individual override CFP's legitimate grounds for processing data

To ask CFP to take any of these steps, you should send the request to hr@assetprotectiongroup.co.uk.

Data Security

CFP takes the security of HR-related personal data seriously and has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties, including internal policies and controls i.e. systems restrictions and IT policy.

Where CFP engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data Breaches

Should CFP discover there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

The organisation will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities

You as an individual are responsible for helping CFP keep your personal data up to date. You should let the HR Department know if data provided changes i.e. should you move house or change bank details.

You may have access to the personal data of other individuals and of our customers and clients in the course of your employment, contract, volunteer period or apprenticeship. Where this is the case, we rely on individuals to help meet our data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation
- to keep data secure (i.e. by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
- not to remove personal data, or devices containing or that can be used to access personal data, from CFP's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to hr@assetprotectiongroup.co.uk immediately

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under CFP's Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing Employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

CFP will provide training to all individuals about their data protection responsibilities as part of the Induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Signature: Date: June 2018

Name: Ashley Haigh Position: Director