Data Protection Policy
GDPR

This document can be made available in other formats on request

Date of Publication	2nd May 2018
Date of Review	May 2020
Policy Author	Daniel Green
Approved By	Martin Green

Rationale

M-Fire Ltd is committed to a policy of protecting the rights and privacy of individuals, including customers and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how companies manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that the company will need to be aware of as data controllers, including provisions intended to enhance the protection of people's personal data. For example, the GDPR requires that: We must ensure that our privacy notices are written in a clear, plain way that people can understand. M-Fire Ltd needs to process certain information about its customers and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. Company / Customer Names
2. Company / Customer Addresses
3. Accounts Contact Names
4. Site Contact Names
5. Accounts and Site Telephone Numbers
6. Accounts and Site Email Addresses

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) M-Fire must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

This policy applies to all customers and other people we may come into contact with whilst fulfilling our duties. Any breach of this policy or of the Regulation itself will be considered an offence and the companies disciplinary procedures will be invoked. As a matter of best practice, other agencies and individuals working with M-Fire and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on the 25th May 2018. The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

Responsibilities Under the GDPR

The Operations Director is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the company.

Compliance with the legislation is the personal responsibility of all employees of the company who process personal information. Individuals who provide personal data to the Company are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found on the ICO's website (www.ico.gov.uk) In order to comply with its obligations, M-Fire undertakes to adhere to the eight principles:

1. **Process Personal Data Fairly and Lawfully**
   The GDPR requires us to process personal data fairly and lawfully. We collect and process data to enable us to provide a service to our customers. M-Fire will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. **Purpose Limitations**
   M-Fire will ensure that the reason for which it collected the data originally is the only reason for which it processes that data, unless the individual is informed of any additional processing before it takes place.

3. **Data Minimisation**
   M-Fire will not seek to collect any personal data which is not strictly necessary for the purpose of which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant is given by individuals, this will be destroyed immediately.

4. **Accuracy**
   M-Fire will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate and each individual should notify the company if, for example, a change in circumstances means that the data needs to be updated. It is the responsibility of M-Fire to ensure that any notification regarding the change is noted and acted on.

5. **Storage Limitations**
   M-Fire undertakes not to retain personal data for longer than is necessary, to ensure compliance with the legislation and any other statutory requirements. This means that M-Fire will undertake a regular review of the information held for as long as necessary.

   M-Fire will dispose of any personal data in a way that protects the rights and privacy of the individuals concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

6. Integrity and Confidentiality

Individuals have various rights under the legislation including a right to:

- Be told the nature of the information M-Fire hold and any parties to whom this may be disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for the purposes of direct marketing.
- Be informed about the mechanics of any automated decision taking process that will significantly affect them.
- Not have significant decisions that will affect them taken solely by automated process.
- Sue or compensation if they suffer damage by any contravention of the legislation.
- Take action to rectify, block, erase or destroy inaccurate date.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened

M-Fire will only process personal data in accordance with individuals' rights.

7. Accountability

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

M-Fire will ensure that all personal data is accessible only to those who have a valid reason for using it.

M-Fire will have in place, appropriate security measures e.g. insuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- Keeping all personal data in a lockable cabinet with key/controlled access.
- Password protected personal data held electronically.
- Archiving personal data which is then kept securely in a controlled access archive store.
- Placing any PC's or Terminals, CCTV monitors etc. that show personal data so that they are not visible to except to authorised staff.
- Ensuring that PC screens are not left unattended without a password protected screensaver being used.

In addition, M-Fire will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as confidential waste and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PC's will be wiped clean before disposal or if that is not possible, destroyed physically.

This policy also applies to staff who process personal data offsite e.g. when working from home or at customer premises, additional care must be taken regarding the security of the data.

8. **Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

   Our Xero accounting software is a cloud-based system and data may be stored on remote servers outside of the EEA. Xero are working towards full compliance by the deadline of the 25th May 2018 and will publish their GDPR-Compliant Data Retention Policy, Data Maps & Data Processing Records before the deadline.

Consent as a Basis for Processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the bet way to ensure that data is collected and processed in an open and transparent manner.

M-Fire does not have a requirement to process any sensitive data as defined by the legislation.

M-Fire understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via an account application form/service agreement).

M-Fire endeavours to contact each customer for whom we hold personal data to request consent moving forward. However due to the nature of our work, we have a responsibility to remind our customers of upcoming inspections and maintenances of fire safety systems, reviews of fire risk assessments and requalification of staff training, therefore if responses to the requests have not been received, the data will be kept until the next scheduled contact where we will attempt to obtain consent again.

Subject Access Requests

Individuals have a right to access any personal data relating to them which are held by the company. Any individual wishing to exercise this eight should apply in writing to the Data Controller. Any member of staff receiving a subject access request should forward this to the Data Controller.

Under the terms of the legislation, any such requests must be complied with within one month and must be available free of charge.

Any disclosure of data must be sent in a commonly used format such as PDF, Excel or Word format. Alternatively, they hard copies can be sent in the post.

Disclosure of Data to Third Parties

M-Fire will not disclose any personal data to third parties for any marketing purposes what so ever.

M-Fire may disclose personal information to selected organisations for the sole purpose of fulfilling the obligations of the service we provide e.g. to sub-contractors who will be required to carry out work on behalf of M-Fire or suppliers who will be required to ship goods direct to the customer.

If required by law, M-Fire may disclose any or all personal data to the police or any government agency requiring it.

Personal Data for Staff and Employees

The policy for how we collect and process personal data of our employees and members of staff is set out in an additional policy.

Procedure for Review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc.

In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.