



General Data Protection Regulation – Policy (And Privacy Statement) **JULY 2020**

Daemon fire and security Ltd – General Data Protection Regulation (GDPR) policy 2019
M. Ryan – MGR Fire and facilities consultants Ltd July 2019
Review date: July 2020 – Next review date: July 2021



General data protection regulation (GDPR) policy:

Key details:

- **Policy prepared by:** M. Ryan (MGR Fire and facilities consultants Ltd)
- **Approved by Directors on:**
- **Policy operational date:**
- **Next review date:**

Introduction:

Daemon fire and security Ltd, needs to gather and use certain information about individuals and organisations, these can include:

- Customers
- Suppliers
- Business contacts
- Employees
- Any other people / organisations having a relationship with the company

Existence of this policy:

This data protection policy ensures that Daemon fire and security Ltd:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach

Data protection law:

The data protection Act 2018 describes how organisations, including Daemon fire and security Ltd, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or in another format. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The data protection Act is underpinned by eight important principles, they are concerned with personal data and ensure that this data must be:

- Processed fairly and lawfully
- Obtained only for specific, lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date

- Processed in accordance with the rights of data subjects
- Protected in appropriate ways

The data must not be:

- Held for any longer than necessary
- Transferred outside of the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope:

This policy applies to the following:

- Head office of Daemon fire and security Ltd
- All staff and volunteers of Daemon fire and security Ltd
- All contractors, suppliers and other people working on behalf of Daemon fire and security Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act (2018).

This information can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals

Data protection risks:

This policy helps to protect Daemon fire and security Ltd from some very real data security risks, including:

- **Breaches in confidentiality** – information being given out inappropriately
- **Failing to offer choice** – all individuals should be free to choose how the company uses data relating to them
- **Reputational damage** – the company could suffer if hackers successfully gained access to sensitive data

Responsibilities:

Everyone who works for or in conjunction with Daemon fire and security Ltd have some responsibility for ensuring data is collected, stored and handles appropriately.

All staff who handle personal data, must ensure that it is handled and processed in line with this policy and data [protection principles.

Individual staff members who key areas of responsibility:

- **The Directors of Daemon fire and security Ltd** - are ultimately responsible for ensuring that the company meets its legal obligations

Daemon fire and security Ltd (or data protection officer, if appointed) is responsible for:

- Reviewing all data protection procedures and related policies are in line with the agreed schedule
- Arranging data protection training and advice for all staff covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Daemon fire and security Ltd holds about them (subject access requests)
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

Daemon fire and security Ltd (or IT manager, if appointed) is responsible for:

- Ensuring that all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services, the company is considering using to store or process data – cloud computing services etc.

Daemon fire and security Ltd (or marketing manager, if appointed) is responsible for:

- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets like newspapers
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General staff guidelines:

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally, when access to confidential information is required, employees can request it from line managers
- Daemon fire and security Ltd, will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines noted
- Strong passwords must be used, and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Data should be regularly reviewed and updated if it is found to be out of date, if no longer required it should be deleted or securely disposed of
- Employees should request help from their line manager or the data protection officer (if appointed), if they are unsure about any aspect of data protection

Data storage:

These rules describe how and where data should be safely stored, questions about storing data safely can be directed to the IT manager (where appointed) or data protection officer (where appointed).

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it.

These guidelines also apply to data that is usually stored electronically but has been printed out for whatever reason:

- When not required, the paper of files should be kept in a secure location
- Employees should make sure that paper and printouts are not left anywhere unauthorised people could access them – a printer for instance
- Data printouts should be shredded and disposed of securely when no longer required

When data is secured electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media (flash drive etc.), these should be stored securely when not in use
- Data should only be stored on designated drives and server, it should only be uploaded to an approved cloud computing service
- Servers containing personal data should be sited in a secure location, away from the general office space
- Data should be backed up frequently, with the backups tested regularly in line with the company's standard backup procedures
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data should be protected by approved security software and a firewall

Data usage:

Personal data is of no value to Daemon fire and security Ltd unless the business can make use of it, however, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally, in particular, it should never be sent by email – this form of communication is not secure
- Data must be encrypted before being transferred electronically, the IT manager (where appointed) can explain how to send data to authorised external contacts
- Personal data should never be transferred outside of the European Economic Area (EEA)
- Employees should not save copies of personal data to their own computers, always access and update the central copy of any data

Data accuracy:

The law requires Daemon fire and security Ltd to take reasonable steps to ensure data kept accurate and up to date.

The more important it is that personal data is accurate, the greater the effort Daemon fire and security Ltd will ensure goes to its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

- Data should be held in as few places as necessary, staff will not create any unnecessary additional data sets
- Staff should take every opportunity to ensure that data is updated, by confirming (for instance), that customers details are confirmed when they call
- Daemon fire and security Ltd, will make it easy for data subjects to update the information the company holds about them, for instance via the company website
- Data should be updated as inaccuracies are discovered, for instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database
- It is the marketing managers (where appointed), responsibility to ensure that marketing databases are checked against industry suppression files every six months

Subject access requests:

All individuals who are the subject of personal data held by Daemon fire and security Ltd are entitled to the following:

- Enquire what information the company holds about them and why
- Ask how to gain access to this information
- Be informed how to ensure that it is kept up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the company requesting information, it is called a “subject access request”.

Subject access requests from individuals should be made by email, addressed to the data protection officer (where appointed), the data protection officer can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request; the data protection officer will aim to provide the relevant data within 14 days of the request.

The data protection officer (where appointed), will always verify the identity of anyone making a subject access request before supplying any information.

Disclosing data for other reasons:

In certain circumstances, the Data Protection Act (2018) allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances Daemon fire and security Ltd will disclose requested data, however, the data protection officer (where appointed) will ensure that the request is legitimate, seeking assistance from the Directors / company’s legal advisers as necessary.

Providing information:

Daemon fire and security Ltd aims to ensure that individuals are aware that their data is being processed and that they understand:

- The data is being used
- How to exercise their rights



To these ends, the company has a privacy statement (appendix A), setting out how data relating to individuals is used by the company, a copy of this statement is available on request.





Policy Acceptance:

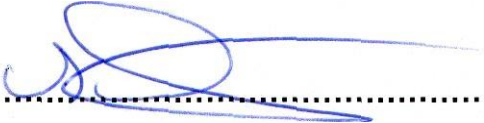
The data protection Act 2018 describes how organisations, including Daemon fire and security Ltd, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or in another format. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Daemon fire & security Ltd, has developed this policy to ensure that it complies with the requirements of the Data Protection Act (2018).

Daemon fire & security Ltd, have prepared the following General Data Protection Policy (GDPR) and all other relevant policies for the protection of all persons having cause to be employed by and work with the company.

The signature below is the acceptance of the Directors to agree its contents and accept its provisions.

SIGNED: 

NAME / POSITION: *Simon Woolton*

DATE: *10-07-2020*

Daemon fire and security Ltd – General Data Protection Regulation (GDPR) policy 2019
M. Ryan – MGR Fire and facilities consultants Ltd July 2019
Review date: July 2020 – Next review date: July 2021



Appendix A

Daemon Fire & Security Limited - Privacy Policy and Notice of Compliance

This Privacy Policy and Notice of Compliance details how Daemon Fire & Security Limited holds and processes personal data in its possession.

Daemon Fire & Security Limited is committed to strengthening its standards and procedures in compliance with both the General Data Protection Regulation 2018 (GDPR) and the Data Protection Act 1998.

We are committed to ensuring that personal data in our possession is protected with information by which you can be identified, whether obtained by electronic or documentary means, or when using our website, will only be used and processed in accordance with this policy.

Collection and Processing of Personal Data:

We may collect and process personal data such as:

- Your name, Company, and job title
- Your contact information, including email addresses
- Other information in relation to potential business activities, such as offers and surveys

The information we hold is entirely for maintaining our trading relationship and communication with you, this information will assist us in providing a better service and addressing OUR customer requirements.

Keeping personal data secure:

In compliance with GDPR, we will ensure that personal data is kept secure, appropriate procedures are in place to prevent unauthorised access, disclosure or distribution.

Third Parties:

We will never sell, distribute, loan or otherwise distribute your personal data to third parties unless we have your permission to do so, or if we are required by law to do so.

We do not use your information for marketing purposes, and we do not share your information with any other third parties.





Data currently held by Daemon Fire & Security Limited:

You may change your mind or amend your preferences regarding your current personal data held by Daemon Fire & Security Limited, at any time. You can do this by emailing us at:

info@daemonfire.co.uk

Alternatively, you can write to us at:

Daemon Fire & Security Ltd, Units 1 & 2, B5K Business Park, Quartz Close,
Tamworth. Staffordshire. B77 4GR
Tel: 01827 69266

