Detect Fire & Security Ltd

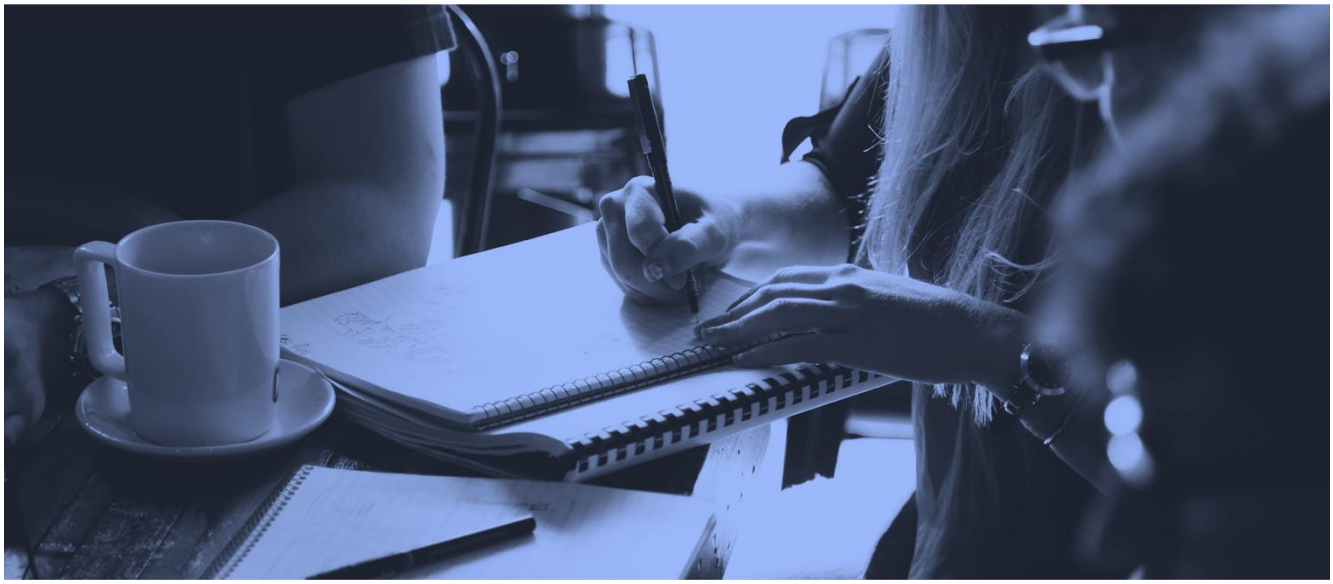
GDPR Compliance Statement

Andrew Derrick
Operations Director

CONTENTS

Executive Summary

Effective from 25th May 2018 the General Data Protection Regulations is a European Law that applies to our organisation relating to the manner in which we store and use personal information (relating to individuals, not companies) We intend to be transparent and cooperative with those individuals affected by our duties under GDPR and our selected partners. Their data will always be used fairly and lawfully.



We have set-out a robust and earnest approach. However, we recognise that during implementation and with the benefit of experience, we may have reason to amend and adapt the policy to reflect broader considerations. As such, this document is considered as a 'living' document and subject to continuous improvement, evolving to meet the appropriate needs under our responsibility.

Version 1
Completed 01/05/2018
Security By: A Derrick

DATA DEFINITIONS

Data that can be used by itself or in combination with other data to identify an individual. Data could be, but is not limited to:

- Name
- Number
- Address
- Other details such as banking etc.

A name, such a Jane Smith may, in itself, not necessarily be classed as personal data since there maybe many Jane Smith's. However, in combination with other data such as an address; that person is then *identified.* Conversely you may not know the name of the person who lives at 10 Hill Rd, however, by approaching 'the tall lady' that lives at 10 Hill Rd, you may be deemed to have identified that person. Where a camera system views a person who can be visually identified by their physical appearance, to an operator or during recorded playback, that too, constitutes personal identification.

What personal data do Detect Fire & security Ltd hold?

- Personnel– Employees & Ex-employees
  - Personal information + family, next of kin etc.
  - Wages
  - Screening, DBS checks, DVLC, previous employment history

- Customers – Domestic (or combined places of work & dwelling)
  - Names of owners of all systems within dwellings
  - Names, addresses, contact details
  - Banking details
  - Keyholders for above

- Customers – non- domestic
  - Individuals representing that business, keyholders

- Suppliers
  - Subcontractors (who work from home)

A category of **Sensitive Personal Data** is defined as 'special categories of personal data' This relates to very specific data that can positively identify an individual, such as: Biometric data (prints, retina scans, DNA swabs etc)

Knowledge and details of a person's previous convictions etc does not fall under this category, however, the management and sensitive maintenance of this data does attract the same high levels of rigor.

RESPONSIBILITY

GDPR protects the rights of individuals whom the data is about (known as 'Data Subjects') by placing duties on those who maintain, store and decide how and why such data is processed.

At the very top of an organisation, someone may be appointed to assume responsibility for the management and accountability for compliance. This person maybe known as: **Data Protection Officer.**

In all other cases (at Detect Fire & security Ltd) the **Operations Director** will assume responsibility for the compliant management under GDPR as follows:

- Maintain the GDPR Policy
- Establish compliant processes
- Measure activity for compliance
- Respond to Data Breaches

Detect Fire & Security Ltd (an organisation) determine what and how we process personal data. This role is known as: **Data Controller.**

Team members (employees) whose job role encompass: using, recording, amending, deleting personal data are known as: **Data Processor.**

A person whose personal data we store and use for our legitimate business purposes is known as the: **Data Subject**.

Certain partners that Detect Fire & security Ltd engage with may also legitimately use our data to fulfill their service to us. They are also known as: **Data Processor.**

Outsourcing certain business functions invoke this third-party Data Controller activity:

- Payroll & Pensions
- Insurances
- Security screening & DBS agencies
- Alarm Receiving Centre's
- Accountants
- Industry training and license registrations
- I.T Support Contractor
- Police Authorities

Where is personal data present?

Data contained within our I.T systems, CRM (CASH) and Accounting systems (SAGE) in electronic form as well as more traditional historic *paper* files and folders within filing cabinets. Back-up and Disaster Recovery Data is located within our physical business domain.

Detect Fire & Security Ltd will NOT share data with third parties for the purposes of advertising and marketing or outsource bulk mail (overland or electronic) Personal data detailed in this document will be solely used for purposes it was originally gathered and recorded.

Personal data managed and used, falls under the categories below:

I.T Systems ~ Security & Access Rights

Through I.T Domain management, password access/protection, regular password resets with prevention of repeat passwords and a structured access table maintained to ensure that only legitimate users can access personal data with permission. Individual workstations will all require a log-in registered to that user, the workstation will auto-sleep after 5 minutes; requiring a log-in to regain access.

I.T is fully supported 24/7. Windows server 2012 R2 is properly patched and backed-up with redundancy. Inbound traffic is routed through a proprietary fire wall before reaching servers which then pass traffic through a proprietary virus guard. Software is legitimately licensed and procured with full audit trail from reputable, registered resellers.

Thin clients are typically <3 years old, have proprietary virus guards and legitimate licensed software.

Remote access is limited to specific users who are registered and who gain access via proprietary App on engineer tablets and /or Citrix. All via fully supported, patched and managed software licenses. Logins and activity leaves an audit trail.

Employee information:

Accessible to legitimate users by login and assigned permissions:

- 2 Directors
- HR Manager
- Finance Controller
- 2 Finance administrators

Management structure:

- SAGE Line 200 with latest software patches, full SAGE support contract; Limited users with unique access rights & permissions – full audit trail.
- Online Banking – Cloud-based; Limited users with unique access rights, dongles & access permissions – full audit trail.
- Personnel – Hard drive devoted to personnel content. Backed-up within the business domain.
- Filing cabinets maintained locked and keys within labelled key safe for legitimate users
- NOTE: *Intention to scan and soft copy all documents to electronic format diminishing need for filing cabinets.*

COMPLIANT WORKING

Customer information:

Accessible to legitimate users by login and assigned permissions:

- Administrators
- Sales Team
- Projects Team
- Service Team
- Finance Team Controller
- Engineers (Tablet)

Management structure:

- SAGE Line 200 with latest software patches, full SAGE support contract; Limited users with unique access rights & permissions – full audit trail.
- CASH (Mentor) with latest software patches, full MENTOR support contract; Limited users with unique access rights & permissions – full audit trail.
- CASH mobile App (Mentor) with latest software patches, full MENTOR support contract; Limited users with unique access rights & permissions – full audit trail. No data stored on-device. App is a portal to the Server (see page 5)
- Filing cabinets maintained locked and keys within labelled key safe for legitimate users
- NOTE: *Intention to scan and soft copy all documents to electronic format diminishing need for filing cabinets.*
- Alarm Receiving Centre – Customer connections + Keyholders

Suppliers - Subcontractors (who work from home)

- Sales Team
- Projects Team
- Service Team
- Finance Team Controller

Management structure:

- SAGE Line 200 with latest software patches, full SAGE support contract; Limited users with unique access rights & permissions – full audit trail.
- CASH (Mentor) with latest software patches, full MENTOR support contract; Limited users with unique access rights & permissions – full audit trail.
- Filing cabinets maintained locked and keys within labelled key safe for legitimate users
- NOTE: *Intention to scan and soft copy all documents to electronic format diminishing need for filing cabinets.*

LAWFUL PURPOSE

The GDPR determines rights for Data Subjects where their consent may be given or implied. Detect Fire & Security Ltd deem the necessity of this data as detailed herein as the 'lawful purpose' to store, manage and utilise this data.

We recognise an individual's right to modify-use or remove their data. They have a right:

- To be informed
- Of access
- Of rectification
- To erasure
- To restrict processing
- To data portability
- To object

The purpose of customer personal data collected and managed within Detect Fire & security Ltd is;

- To compliantly administer the sales, installation, servicing and repair of electronic fire & security systems.
- Meet the expectations of published standards, UK Law, Governing/Regulatory Bodies, Codes of Practice.
- A minimal amount of data will be maintained to fulfill legal, industry guidelines and financial administration of these activities.

The nature and necessity of personal data gathered is determined within CRM (CASH) and managed in such a way that essential fields *must* be completed before being permitted to move-on to other fields. It is deemed that this encourages minimal data to be been recorded.

Members of staff who are requested; by an employee or customer for any of the above are instructed to refer to the Operation Director for consent and support, before any data is discussed or amended in any manner.

Save the necessity of record keeping in compliance with our governing bodies and regulatory authority (who we deem as superior to GDPR) we will recognise and collaborate openly with anyone exercising their rights to above.

PARTNER STATEMENTS

Our partners and business connections enable us to maintain industry compliance in areas where our specific expertise such as:

- National Security Inspectorate. Connection of intruder and fire alarm systems.
- Relationships with the Police and Fire & Rescue services.
- Accountants for payroll and HMRC compliance
- Accounting software to maintain HMRC requirements (SAGE)
- Specialist I.T support services (Peach Technology)
- CRM and back-office software (Mentor – CASH)
- Operating software & systems (Microsoft)
- Alarm Receiving Centre – System connections (Southern Monitoring & SecuriGaurd)
- Financial advice and management of Pensions, Insurances etc (Independent Financial Solutions)
- Health & Safety compliance (Watson & Watson)

We maintain on record the individual GDPR Policy documents for each of these partners with whom we may have necessity to exchange your personal information.