PRIVACY POLICY

KELVIN FRANCIS DATA PROTECTION POLICY

Key Details

- Policy prepared by: Tony Filice
- Approved by Directors on 3 April 2017
- Policy becomes operative on 4 April 2017
- Next review date 21 January 2023

Rationale

Our data protection policy, sets out our commitment to protect personal data and how we implement that commitment, with regard to the correction and use of personal data.

We are committed to:

- Ensure that we comply with the eight Data Protection Principles as listed below.
- Meeting our legal obligations as laid down by the Data Protection Act 1998.
- Ensuring that data, is collected and used fairly and lawfully.
- Processing personal data, only in order to meet our operational needs, or fulfil our legal requirements.
- Taking steps to ensure that personal data is up to date and accurate.
- Establishing appropriate retention periods for personal data.
- Ensuring that data subjects' rights can be appropriately exercised.
- Providing adequate security measures to protect personal data.
- Ensuring that a nominated officer is responsible for data protection compliance and providing a point of contact for all data protection issues.
- Ensuring that all staff are made aware of good practice in data protection.
- Providing adequate training for all staff responsible for personal data.
- Ensuring that everyone handling personal data, knows where to find further guidance.
- Ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly.
- Regular reviewing of data protection procedures and guidelines within the organisation.

Data Protection Principles

The eight data protection principles are laid down in the 1998 data Protection Act which must be followed at all times:-

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained, only for one or more specific and lawful purpose and shall not be further processed, in any other manner incompatible with that purpose, or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose, or purposes, for which it is processed.
4. Personal data shall be accurate, where necessary, kept up to date.
5. Personal data processed for any purpose, or purposes, shall not be kept for longer than is necessary for those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects, under the 1998 Data Protection Act.
7. Appropriate technical and organisational measures, shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country, or territory, ensures an adequate level of protection for the rights and freedoms of data subjects, in relation to the processing of personal data.

Policy Scope

This policy applies to:-

- All branches of Kelvin Francis Sales and Rentals.
- All staff and volunteers of Kelvin Francis Sales and Rentals.
- All contractors, suppliers and other people working on behalf of Kelvin Francis.

It applies to all data the Company holds, relating to identifying all individuals, even if that information technically falls outside the Data Protection Act 1998. This 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 Kelvin Francis from some real security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the Company uses data relating to them.
- **Reputational damage**. For instance, the Company reputation could suffer, if hackers successfully gained access to sensitive data.

The Responsibilities

Everyone who works for or with Kelvin Francis Sales or Rentals, has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data, must ensure that it is handled, and processed in line with this policy and data protection principles.

General Staff Guidelines

- The only people to access data covered by this policy, should be those who need to do so for their work.
- Data should not be shared informally. When access to confidential information is required, employees must request it from the higher managers.
- Kelvin Francis will provide training to all employees, to help them understand their responsibilities for handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and these should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Company, or outside it.
- Data should be regularly reviewed and updated if it is found to be out of date. If not longer required, it should be deleted and securely disposed of.
- Employees should request help from their Office Managers, or their Data Protection Officer, (Tony Filice), if they are unsure of 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 Data Protection Officer.

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

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

- When not required, the paper or files, should be kept in a **locked drawer or filing cabinet.**
- Employees should make sure paper and print outs are **not left where unauthorised people can see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely, when no longer required.

When data is stored 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** (like CD or DVD), these should be kept locked away securely, when not being used.
- Data should only be used on **designated drives and servers** and should only be uploaded in approved Cloud computing services.
- Servers containing personal data should be **sighted in a secure location**, away from general office area.
- Data should be **backed up frequently**. Those back ups should be tested regularly, in line with the Company standard back up procedures.
- Data should **never be saved directly** to laptops, or other mobile devices, like tablets or smartphones.
- All servers and computers containing data, should be protected by **approved security software and a firewall**.

Data Use

Personal data is of no value to Kelvin Francis 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 that **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, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT Managers can explain how to use data to unauthorised external contacts.
- Personal data should **never be transferred outside of the European economic area.**
- 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 Kelvin Francis to take responsible steps, to ensure data is kept accurate and up to date.
The more important it is, that the personal data is accurate, the greater the effort Kelvin Francis should put into ensuring its accuracy.
It is the responsibility of all employees who work with data, to take reasonable steps to ensure it is kept accurate and up to date as possible.

- Data will be held in as **few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming customers details, when they call.
- Kelvin Francis will make it easy for data subjects to update the information Kelvin Francis 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 Directors responsibility to ensure **marketing databases are checked against industry suppression files** every 6 months.

Subject Access Requests

All individuals who are the subject of personal data held by Kelvin Francis are entitled to:

- Ask what information the Company holds about them and why?
- Ask how to gain access to it?
- Be informed how to keep it up to date?
- Be informed how the Company is meeting its Data Protection obligations?

If an individual contacts the Company requesting this information, this is called a **subject access request.**

Subject access request from individuals should be made by email, addressed to the Data Controller email tony@kelvinfrancis.com

Individuals will be charged £10.00 per subject access request. The Data Controller will aim to provide the relevant data within 14 days.

The Data Controller will always verify the identity of anyone making a subject access request, before handing over any information.

Disclosing Data For Other Reasons

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

Under these circumstances, Kelvin Francis will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the Directors and from the Company's legal advisors where necessary.

New EU Data Protection Laws will apply from the 25 May 2018

In May 2018, the General Data Protection Regulation (GDPR) will become law. Despite Brexit, businesses that hold any piece of information about any EU citizen, or do business in the EU, will be impacted by GDPR. It is enforceable regulation, that is applicable to every UK business, regardless of size or market.

What you need to know

If your business loses data, has been negligent, or suffered a service attack, malicious or internal hack, that puts people's rights at risk, it must notify the Data Protection Authority (the Information Commissioner's Office) and the people that are affected **within 72 hours of becoming aware of it.** Should this 72 hour deadline not be met, your business could be fined up to 10 million Euros, or 2% of annual turnover, whichever is greater.