Evans Harvey
Solicitors

Evans Harvey Limited

Data Protection Policy

(incorporating Data Retention and Data Subject Access Policies)

29/3/2018

Data Protection Policy – Evans Harvey Limited

Key details

- Policy prepared by: Deborah Best, Office Manager
- Approved by Director/Data Protection Manager (Stephen Hall) on: 29 March 2018
- Policy became operational on: 29 March 2018
- Next review date: 29 March 2019

Introduction

Evans Harvey Limited needs to gather certain information about individuals.

These can include clients, business contacts, employees and other people the company has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

- This data protection policy ensures Evans Harvey Limited:
- 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 individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulations and Data Protection Act 2018 (hereafter jointly referred to as 'GDPR') describes how organisations – including Evans Harvey Limited – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important in principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Evans Harvey Limited
- All staff of Evans Harvey Limited
- All people contracted or working on behalf of Evans Harvey Limited

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. 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 Evans Harvey limited from some very real data 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 could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for Evans Harvey Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each staff member who handles personal date must ensure that it is handled, processed and stored in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Director/Data Protection Manager ('DPM') is ultimately responsible for ensuring that Evans Harvey Limited meets it legal obligations

- The Office Manager will assist the DPM by:

  - Keeping the DPM updated about data protection responsibilities, risks and issues
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule
  - Arranging data protection training and advice for the people 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 Evans Harvey Limited holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

  Plus, in conjunction with Cutec Ltd, be responsible for:

  - Ensuring 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 third-party services the company is considering using to store or process data. For instance, cloud computing services

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.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, **strong passwords** must be used and they should never be shared. Staff however are required to inform the Office Manager of their passwords, who will record same within an encrypted document.

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 and disposed of

Employees should request help from their Head of Department or the Office Manager if they are unsure about any aspect of data protection

Data storage

These rules describe how and where data should be safely stored.

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 printouts are not left where unauthorised people could see them. For example, the reception area.
- 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 (other than as set out above)

If data is stored on removable media (like CD or DVD), these should be **kept locked away** securely when not being used

Servers containing personal data should be sited in a secure location, away from general office space

Data should be **backed by frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures

Data should **never be saved directly** to laptops or other mobile devised like tablets or smart phones.

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 Evans Harvey Limited unless the business can make use of it or they are obliged to obtain same under the Money Laundering Regulations 2007. When personal data is accessed and used 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 unless it is encrypted, as this form of communication is not secure

Data **must be encrypted before being transferred electronically**. The Office Manager can explain how to encrypt data is necessary.

Employees should **not save copies of personal data to their own computers**. Always access and update the **central copy of any data** and store client information and documents **only in the relevant client folders on the Z drive. Client information must not be stored in any other folder.**

Data accuracy

The law requires Evans Harvey Limited to take reasonable 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 Evans Harvey Limited should put into ensuring its accuracy

It is the responsibility of all employees who work with the data to take reasonable steps to ensure it is kept as 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 a customer's details when they call
- Data should be **updated as inaccuracies are discovered**. For instance, if a client can no longer be reached by their stored telephone number, it should be removed from the database

Subject access requests

All individuals who are the subject of personal data held by Evans Harvey Limited are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be information how to keep it up to date (if applicable)
- 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 requests from individuals should be made by email, address to the Office Manager at deborahbest@evansharvey.co.uk. The Office Manager can supply a standard request form although individuals do not have to use this.

The Office Manager will aim to provide the relevant data within 30 days.

The Office Manager 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 GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances Evans Harvey Limited will disclose requested data. However the Office Manager will ensure the request is legitimate, seeking assistance from the Director and from legal advisers where necessary