Company Policy

For

GDPR

Introduction

GDPR is a new EU regulation which comes into force on the 25 May 2018, this replaces the 1998 Data Protection Act.

Hanover Insolvency Limited needs to gather and use certain information about individuals. These can include customers, suppliers, business contracts, employees and other people the organisation has a relationship with or may need to contact.

Why this policy exists

- Comply with the EU 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 risk of a data breach

The key principles are

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

Policy Scope

Applies to:

- All office's of Hanover Insolvency Limited
- All staff and volunteers of Hanover Insolvency Limited
- All contractors, suppliers and other people working on behalf of Hanover Insolvency Limited

It applies to all data that the company holds relating to identifiable individuals this can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

Risks, Responsibilities and People

Risks

- This policy helps to protect Hanover Insolvency 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 or with Hanover Insolvency Limited has 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 the policy and the key principles.

The Compliance Manager is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all policies and procedures
- Arranging 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 subject access requests
- Responding to requests for rectification and Erasure

The Operations Manager is 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 any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
- 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 their line managers.
- **Hanover Insolvency Limited 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 below.
- 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 and disposed of.
- Employees **should request help** from their line manager or the compliance manger if they are unsure about any aspect of GDPR.

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.
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,** 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 password** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD, DVD or memory pen), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers,** and should only be uploaded to an **approved cloud computing service.**
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up 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 mobiles devices 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 Hanover Insolvency Limited 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, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically.** The IT Director can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area,** except where we work with a **business partner** to enable us to provide you with our services and they will process information outside of the EEA.
- If we do share your information outside of the EEA we will make sure that it is **protected** in the same way as if it was being used in the EEA.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data Breach

Hanover Insolvency is required to notify the ICO of a data breach within 72 hours of it occurring.

- Staff are aware that they should notify the Compliance Manager of any data breaches.
- A process is in place to make any individuals affected aware should a data breach occur.
- All possible precautions are made to ensure that data breaches don't happen.
- The Compliance Mangers will notify the ICO of a data breach.

Data Accuracy

The law requires Hanover Insolvency Limited to take reasonable steps to ensure data is accurate and kept up to date.

The more important it is that the personal data is accurate, the greater the effort Hanover Insolvency Limited should put into ensuring its accuracy.

It is the responsibility if all employees who work with 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.
- Hanover Insolvency Limited will make it **easy for data subjects to update the information**

- 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.

Subject Access Requests

All individuals who are the subject of personal data held by Hanover Insolvency Limited 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 obligations.**

When 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, addressed to the Compliance Manager at Nicola.whitham@hanoverinsolvency.co.uk. The Compliance Manager can supply a standard request form, although individuals do not have to use this.

The Compliance Manager will aim to provide the relevant data within one month.

The data controller (in this instance the Compliance Manager) will always verify the identity of anyone making a subject access request before providing any information.

Rectification & Erasure

All individuals who are the subject of personal data held by Hanover Insolvency Limited are entitled to request a rectification or erasure of the data that is held by the company.

Requests from individuals should be made by email, addressed to the Compliance Manager Nicola.whitham@hanoverinsolvency.co.uk.

The Compliance Manager will aim to respond to such a request within one month.

Special Category Data

There will be some occasions when Hanover Insolvency staff will need to obtain and process special category data information relating to previous or current health conditions.

Staff will gain explicit consent from the individual and they will be made aware of where this information will be held and for what purpose.

Disclosing Data for Other Reasons

In certain circumstances, personal data can be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Hanover Insolvency Limited will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's compliance manager.

Providing Information

Hanover Insolvency Limited aims to ensure that individuals are aware that their data is being processed, and that they understand:

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

To these ends, the company has a privacy policy, setting out how data relating to individuals is used by the company this is visible on the Hanover Insolvency website.

PEOPLE, RISKS AND RESPONSIBILITIES

Policy Scope

This policy applies to:

- The head office of Hanover Insolvency Limited
- All branches of Hanover Insolvency Limited
- All staff and volunteers of Hanover Insolvency Limited
- All contractors, suppliers and other people working on behalf of Hanover Insolvency Limited

This policy will be reviewed regularly and was last updated in March 2021.