

# DATA PROTECTION POLICY

## CONTEXT AND OVERVIEW

### Key details

- Policy prepared by: Alan Rhodes and Karla Swain
- Approved by: Mark Henderson
- Policy became operational on: February 1<sup>st</sup> 2015
- Review Date: Annually

### Introduction

Magicman Limited needs to gather and use certain information about individuals to meet its operational needs. These individuals include employees, customers, suppliers, business contacts and any other people the company has a relationship with or may need to contact.

This policy sets out Magicman Limited’s commitment to protecting personal data in accordance with its legal obligations as laid down in the General Data Protection Regulation (GDPR) and how it implements that commitment with regards to the collection and use of personal data.

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

Magicman Limited takes the privacy of its employees, customers, business contacts and all other interested parties very seriously investing significant resources as part of our efforts to protect the personal data that we store adhering always to the applicable privacy rules. Our Privacy Policy describes how we work to maintain that trust and protect all those whose information we hold.

### Why this policy exists

This data protection policy ensures Magicman Limited:

- Complies with the General Data Protection Regulation and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open and transparent about how it stores and processes the data of individuals.
- Protects itself from data breach.

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---

## GDPR

The GDPR is a regulation passed by the European Union (EU), effective from 25<sup>th</sup> May 2018, that relates to the protection of the personal data of individuals, such as their names, email addresses, phone numbers, identification numbers etc. This regulation will provide more rights and protections to individuals. It also places more obligations on businesses when it comes to transparency, security and accountability in processing personal data.

Magicman Limited is committed to ensuring that it complies with the principles in Article 5 of GDPR which state that data should be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Retained only for as long as necessary
- Proposed in an appropriate manner to maintain security

Furthermore, Magicman Limited will ensure that:

- A nominated officer is responsible for data protection compliance and to provide a point of contact for all data protection issues.
- All Magicman Limited staff are made aware of good practice in data protection.
- Adequate training shall be provided for all staff responsible for personal data to ensure that they are aware of good practice in data protection.
- It will ensure that everyone handling personal data knows where to find further guidance.
- It will ensure queries about data protection, internal and external to the organisation, are dealt with effectively and promptly.
- It will regularly review data protection procedures and guidelines within the organisation.

## PEOPLE, RISKS AND RESPONSIBILITIES

### Policy scope and the people it applies to

This policy applies to:

- The Head Office of Magicman Limited.
- All staff of Magicman Limited.
- All contractors, suppliers and any other people working on behalf of Magicman Limited.
- Magicman Global Licensing Limited.

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of GDPR. This includes:

- Names of individuals
- Postal addresses
- Email addresses
- Damage photographs
- Telephone numbers
- Any other information relating to individuals

We will continue to increase transparency and communication with our users to provide you with as clear an understanding as possible about how your personal data is processed. We will facilitate the right of individuals introduced by GDPR, including the rights of individuals to access and / or delete their personal data upon request. We will remain dedicated to the approach of ‘privacy by design and default’ through the consistent application of the privacy principles in the GDPR, and the adoption of a privacy-friendly approach in how we build and operate our products and services.

**Data protection risks**

This policy helps to protect Magicman Limited from data security risks including:

- **Breaches of confidentiality** such as information being given out inappropriately.
- **Failing to offer choice.** Individuals should be free to choose how their personal data is used.
- **Reputational damage** caused by unauthorised or illegal access.

**Responsibilities**

Everyone who works for or with Magicman Limited shares some responsibility for ensuring data is collected, handled and stored appropriately. Each team that handles personal data must ensure that data is handled and processed in compliance with this policy and the principles in Article 5 of GDPR.

However, the following people have key areas of responsibility:

- **Chief Executive Officer**, Mark Henderson is responsible for:
  - Ensuring that Magicman Limited meets its legal obligations.
  - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
- **Customer Care Co-Ordinator**, Danielle Millard-Ackred, is responsible for:
  - Keeping Director updated about data protection responsibilities, risks and issues.
  - Reviewing data protection procedures and policies within an agreed schedule.

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---

- Arranging data protection training and advice for Magicman Limited staff.
- Handling data protection questions.
- Dealing with data requests, also known as ‘subject access requests’, from individuals asking to see the data Magicman Limited holds about them.
- **IT manager**, Andrea Pompili 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 may considering using to store or process data including cloud computing services.
- **Blue Chip**, provider of Cloud Storage, is responsible for:
  - Physical security of hosting services
  - Secure access to support services
- **Marketing & Communications Manager**, Alan Rhodes 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.
  - Working with staff to ensure marketing initiatives abide by data protection principles.

## GENERAL STAFF GUIDELINES

1. Access to data covered by this policy should be restricted to include only information necessary for their work.
2. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
3. Magicman Limited will provide training to all employees to help them understand their responsibilities when handling data.
4. Employees should keep all data secure by taking sensible precautions and following the guidelines below.
5. Strong passwords must be used and should never be shared.
6. Data should not be accessed in public spaces using unsecured Wifi networks.
7. Data should be reviewed and updated if it is found to be out of date. If no longer required, it should be deleted or disposed of.
8. Employees should request help from their line manager 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 or Customer Care Co-Ordinator.

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---

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 printed out.

- 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 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 frequently and never shared between employees.
- If data is stored on removable media like a CD, DVD or USB stick, these should be locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from the general office space.
- 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 security software and a firewall.

How does Magicman Limited manage personal data transfers?

- All data is stored and transferred only within the UK

## DATA ACCURACY

The law requires Magicman 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 Magicman Limited 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 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.

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---

- Magicman Limited will make it easy for data subjects to update the information Magicman Limited hold about them, for instance via the company website.
- Data should be updated as inaccuracies become apparent. For example: a telephone number that no longer works should be removed from the database.

## **SUBJECT ACCESS REQUESTS AND THE RIGHT TO BE FORGOTTEN**

All individuals who are the subject of personal data held by Magicman 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 protection obligations.

If an individual contacts Magicman Limited requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the HR Administrator, Samantha Lane via email to [hr@magicman.co.uk](mailto:hr@magicman.co.uk) The HR Administrator and can supply a standard request form, although individuals do not have to use this.

This is a free service and the HR Administrator will aim to provide the relevant data within one calendar month. The HR Administrator will always verify the identity of anyone making a subject access request before releasing any data.

Should you wish for Magicman Limited to delete the information that you have previously consented for us to hold under the Article 17 GDPR Right to Erasure 'Right to be Forgotten' please notify the Customer Care Team via email to [customercare@magicman.co.uk](mailto:customercare@magicman.co.uk) .

## **COMPLAINTS PROCEDURE**

If you wish to make a complaint about how your personal data has been used when held by Magicman Limited, how it was collected, its accuracy or for any other reason, please email the Customer Care Team, on [customercare@magicman.co.uk](mailto:customercare@magicman.co.uk) outlining the nature of your complaint and providing any evidence to support inaccuracies. The Customer Care Team will make every endeavour to resolve your complaint within 7 days.

## **DISCLOSING DATA FOR OTHER REASONS**

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

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---

Under these circumstances, Magicman Limited will disclose requested data. However, the company will ensure the request is legitimate, seeking assistance from the Company Directors and their legal advisors where necessary.

### PROVIDING INFORMATION

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

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

### Phone Calls

All incoming and outgoing calls to landlines in our offices are recorded for quality and training purposes and for the protection of employees and customers. Call recordings are paused and the customers notified during financial transactions to ensure that information such as bank account and credit card details are not captured.

### Customer Photos

Magicman Limited request that potential customers provide digital photographs of damaged areas or items for costing and technical evaluation. Photographs are stored digitally on a virtual server hosted by Amazon Web Services in such a manner that the customer and his or her address cannot be identified without the association of Magicman Limited's Customer Relation systems which are hosted by Blue Chip in another location.

### Direct Marketing

Magicman Limited does not sell, rent or share personal data collected will not be sold on to third parties outside the company for the purposes of direct email or telemarketing.

### CCTV

For the security of Magicman staff and stored data we have in place a 24-hour CCTV security system.

No more images and information are stored than that which is strictly required for the purpose of a surveillance camera system, and such images and information are deleted once their purposes have been discharged. Access to retained images is restricted and disclosure of images and information will only take place when it is necessary for such a purpose or for law enforcement purposes.

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---

<b>Prepared By</b> Karla Swain	<b>Reviewed By</b> Martyn Howells	<b>Approved By</b> Mark Henderson	<b>Issue: 04 Version 01</b> May 2018
-----------------------------------	--------------------------------------	--------------------------------------	---