Hardy Signs Limited

Data Controller

Document Version 7.1

Data Audit: 6 May 2026

ICO REGISTRATION NO: ZA 242282

C O R P O R A T E
R E S P O N S I B I L I T Y:-

NICHOLAS HARDY
Data Protection Manager

DATA PROTECTION MANAGEMENT SYSTEM

Online Privacy Notice

HARDY SIGNS LIMITED

Registered Member of the GDPR Check & Verify Register

www.gdprcheckandverify.com

1 COMPANY CONTACT DETAILS

1.1 Hardy Signs Limited The Maltsters, Wetmore Rd, Burton upon Trent DE14 1LS hereinafter referred to as 'the Company', We, Us and Our.

1.2 Our email address is: n.hardy@hardysigns.co.uk

1.3 Our contact telephone number is: 01283 569102

1.4 We are a Data Controller under the provisions of the UK GDPR and the Data Protection Act 2018 and have registered with the UK Information Commissioners office:

ICO Registration Number: ZA 242282

2 Status of key personnel

2.1 We have designated **Mr Nicholas Hardy** as **Data Protection Manager** for the business.

2.2 Please direct any data protection queries to the email address above.

3 INTRODUCTION AND OVERVIEW

3.1 This Privacy Notice explains how we collect, use and protect personal data when you

a) visit our website

b) contact us

c) buy products or services from us

d) otherwise interact with us

3.2 We are committed to protecting your personal information and complying with UK data protection law.

3.3 Further internal policies and procedures support our compliance with UK data protection law.

4 SCOPE OF THIS PRIVACY NOTICE

4.1 This Privacy Notice applies to Personal Data we process when you visit or use our website. Further Privacy Policy statements and documents may apply offline and these are available, if relevant, on request.

4.2 We have described below the personal information we may gather about you, the purposes we will hold it for and the limited categories of people to whom we may disclose it.

5 THE PERSONAL DATA WE PROCESS

5.1 During your visit to our site, we will only collect personal information that you choose to provide. If, for example, you contact us with an enquiry or request us to provide you with further information.

5.2 Where you provide us with another person's data you must ensure you have the authority to do so.

5.3 Depending on how you interact with us, we may process:

a) identity data (e.g. name);

b) contact data (e.g. address, email, telephone number);

c) financial and transaction data;

d) technical and usage data relating to website use;

e) marketing and communications data;

f) employment or recruitment data (where applicable).

We may also process limited special category data where necessary and lawful to do so.

6 HOW WE USE PERSONAL DATA

6.1 We use personal data for purposes including:

a) responding to enquiries;

b) providing products or services;

c) managing contracts and business relationships;

d) communicating with individuals;

e) maintaining website functionality and security;

f) complying with legal obligations;

g) protecting our business, staff, customers, and visitors.

7 LAWFUL BASES

7.1 We process personal data under one or more of the following lawful bases:

a) consent;

b) contract;

c) legal obligation;

d) legitimate interests;

e) vital interests;

f) public task (only if applicable).

7.2 Where we rely on legitimate interests, we carry out appropriate assessments and safeguards.

7.3 Further information regarding legitimate interests processing is available in the ANNEX to this document.

8 MARKETING COMMUNICATIONS

8.1 We may send Marketing communications where permitted by law including where:

a) Consent has been provided; or

b) Where the 'Soft opt in' provisions apply

8.2 Individuals may opt out of marketing communications at any time.

9 DATA SHARING

9.1 We may share personal data with:

a) service providers and data processors;

b) professional advisers;

c) regulatory, legal, or public authorities where required;

d) IT and communication providers.

9.2 We only share personal data where necessary and appropriate safeguards are in place.

10 INTERNATIONAL TRANSFERS

10.1 Where personal data is transferred outside the United Kingdom, we will ensure that appropriate safeguards are in place in accordance with UK data protection law.

10.2 Under UK data protection law, personal data may only be transferred outside the UK where one of the following applies:

(a) The destination country or organisation is subject to a UK adequacy regulation; or

(b) Appropriate safeguards are in place;

(c) A UK International Data Transfer Agreement (IDTA)

(d) An addendum to UK SCCs; or

(e) A limited statutory exception applies.

10.3 The Main Establishment for all of our Data Processing is the UK.

10.4 The competent supervisory authority is the UK Information Commissioner's Office (ICO). whose address is Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

11 DATA RETENTION

11.1 We retain personal data only for as long as necessary for the purposes for which it was collected, including legal, regulatory, accounting, or operational requirements.

11.2 Further information regarding retention periods is available on request.

12 DATA SECURITY

12.1 We use appropriate technical and organisational measures to protect personal data against unauthorised access, loss, misuse, or disclosure.

13 YOUR RIGHTS

13.1 Under UK data protection law, individuals have rights including:

a) the right to be informed;

b) the right of access;

c) the right to rectification;

d) the right to erasure;

e) the right to restrict processing;

f) the right to object;

g) the right to data portability;

h) rights relating to automated decision-making.

13.2 Requests relating to personal data rights may be made using the contact details above.

14 AUTOMATED DECISION MAKING

14.1 We do not carry out solely automated decision-making producing legal or similarly significant effects on individuals.

15 CHILDREN AND SAFEGUARDING

15.1 We recognise that personal data relating to children and safeguarding matters requires additional protection.

15.2 Where we process such data, we do so lawfully, proportionately, and with appropriate safeguards.

15.3 We will not knowingly collect information from persons under 13 years of age without their parent's or guardian's consent.

15.4 There is nothing on our Website which could be damaging to children who view the pages or the pictures.

16 COOKIES

16.1 Our website may use cookies and similar technologies.

What Are Cookies

16.2 Cookies are small text files that are placed on a user’s device when they visit a website. They are widely used to make websites work efficiently, improve user experience, and provide information to website operators.

16.3 Cookies may be:

a) Session cookies, which expire when the browser is closed; or

b) Persistent cookies, which remain on the device for a set period or until deleted.

How We Use Cookies

16.4 We use cookies to:

a) Ensure the website functions correctly

b) Maintain security and prevent fraud

c) Remember user preferences

d) Understand how the website is used, in order to improve performance and content

16.5 Cookies may be set by us ("first-party cookies") or by third parties providing services on our behalf ("third-party cookies").

Managing Cookie Preferences

16.6 Users can manage or withdraw their cookie preferences at any time by:

a) Using the cookie settings tool available on the website; and/or

b) Adjusting browser settings to block or delete cookies

Please note that blocking certain cookies may affect website functionality.

17 BUSINESS SALE OR TRANSFER OF OWNERSHIP

17.1 In the event our business, or part of it, is taken over, bought or merged with another business If our business is sold or reorganised, personal data may be transferred as part of that process, subject to appropriate safeguards.

18 COMPLAINTS

18.1 If you are unhappy with how we process personal data, please contact us using the details above.

18.2 You also have the right to complain to the Information Commissioner's Office (ICO): www.ico.org.uk

19 CHANGES TO THIS PRIVACY NOTICE

19.1 This Privacy Notice may be updated from time to time to reflect changes in law, guidance from the Information Commissioner's Office (ICO), or changes to our use of cookies.

19.2 The latest version will always be available on our website.

19.3 There may be developments in how we use your data according to changes in the Law.

19.4 We reserve the right to make changes to this Data Protection and Privacy Policy, it is your responsibility to revisit this page from time to time to re-read this policy including any and each time you visit our website.

19.5 Any revised terms shall take effect as at the date of posting.

19.6 If you don’t find your concern addressed here, feel free to contact us by e-mailing our Data Protection Manager at the contact details given above.

ANNEX A – LEGITIMATE INTERESTS ASSESSMENTS (LIAs)

This Annex forms part of our Data Protection Management System (DPMS) and contains all current Legitimate Interests Assessments we rely upon.

Each LIA is approved by the Data Protection Manager and is reviewed annually.

LIA-01 – SOFT OPT IN

1 Processing Description

Limited personal data (e.g. name, email address, telephone number) is used to send electronic marketing communications to existing customers or enquirers regarding similar products or services.

2 Purpose Test

• to promote relevant products or services to existing customers;
• to maintain ongoing customer relationships;
• to support business development through proportionate marketing.

3 Necessity Test
• electronic communication (e.g. email/SMS) is an efficient and appropriate method of contact;
• contact details are obtained directly from individuals during a sale or enquiry;
• communications are limited to similar products or services;
• individuals are given a clear opportunity to opt out at the point of data collection and in every message.

4 Balancing Test

Nature of Data
Basic contact details (e.g. name, email address, telephone number).

Reasonable Expectations
Individuals would reasonably expect to receive communications relating to similar products or services following a purchase or enquiry.

Impact
Minimal, as:
• communications are limited in scope and frequency;
• individuals can opt out at any time;
• no special category data is used;
• data is not shared with third parties for marketing purposes.

Risks to individuals
The following potential risks to individuals have been identified:
• unwanted or excessive communications;
• loss of control over personal data;
• distress or inconvenience.

Safeguards
• clear opt-out provided at data collection and in every communication;
• suppression lists maintained and respected;
• prompt action taken on unsubscribe requests;

• access to data is restricted to authorised personnel;
• data is stored securely and protected by appropriate technical measures;
• retention periods are limited;
• staff are trained in data protection requirements;
• policies and procedures govern the use of the data.

Proportionality (DUAA)
Processing is limited to existing customers or enquirers, restricted to similar products or services, and includes clear and ongoing opt-out mechanisms. The processing is controlled and proportionate to a low-impact purpose.

Conclusion
The processing is justified under Legitimate Interests and is carried out in compliance with the Privacy and Electronic Communications Regulations.

Approval and Review

Approved by: Data Protection Manager at the latest Data Audit

Review Date: Next Data Audit

This assessment will be reviewed periodically and where there is a material change to the processing activity.

LIA-02 – VIDEO CONFERENCING

1. Processing Description

We use third-party video conferencing platforms to facilitate communication between staff, clergy, and stakeholders. In some cases, meetings may be recorded.

2. Purpose Test

Processing is necessary to:

- facilitate efficient communication across geographically dispersed participants;
- support operational and administrative activities;
- reduce the need for travel.

These are legitimate organisational interests.

3. Necessity Test

The RB considers that:

- video conferencing is the only practical method for real-time multi-party communication with visual content;
- alternative methods (e.g. telephone) are insufficient where visual information is required;
- use of such platforms is standard and expected in modern organisational operations.

4. Balancing Test

Nature of Data

Audio, video, and limited identifying information.

Reasonable Expectations

Participants would reasonably expect data processing when joining video calls.

Impact

Limited, as:

- recording is not routine;
- participants are informed where recording occurs;
- alternative participation (e.g. audio-only) may be offered where appropriate.

Risks to individuals

The following potential risks to individuals have been identified

- loss of confidentiality;
- unauthorised access to personal data;
- misuse of personal data;
- distress or loss of privacy.

Safeguards

The RB applies the following safeguards to mitigate identified risks:

- platform security settings configured;
- access controls applied;
- recordings retained only where necessary;
- data handled in accordance with RB policies.
- Access to data is restricted to authorised personnel;
- data is stored securely and protected by appropriate technical measures;
- retention periods are limited;
- staff are trained in data protection requirements;
- policies and procedures govern the use of the data.

These measures reduce the likelihood and impact of identified risks.

5. Proportionality (DUAA)

Processing is targeted, limited, and proportionate to its purpose. No less intrusive method would achieve equivalent outcomes.

6. Conclusion

The RB has determined that processing is necessary, proportionate, and does not override the rights of individuals. Legitimate Interests is therefore an appropriate lawful basis.

7. Approval and Review

Approved by: Data Protection Manager at the latest Data Audit

Review Date: Next Data Audit

This assessment will be reviewed periodically and where there is a material change to the processing activity.

LIA-03 – CCTV MONITORING

1. Processing Description

The RB operates Closed Circuit Television (CCTV) systems at its premises to capture visual images of individuals within defined areas.

The system operates on a **passive recording basis**, with footage accessed only where required.

2. Purpose Test

The purposes of the processing are:

- to ensure the safety and security of staff, visitors, and property;
- to prevent and detect crime;
- to assist in the investigation of incidents;
- to support compliance with health and safety obligations.

These purposes are legitimate organisational interests and align with the RB's duty of care and safeguarding responsibilities.

3. Necessity Test

The use of CCTV is considered necessary because:

- visual recording is the only effective means of capturing real-time incidents;
- alternative measures (e.g. manual supervision or written records) would not provide equivalent evidential value;
- the system operates in a targeted manner, covering only relevant areas;
- recording is limited to what is required to achieve the stated purposes.

The RB has determined that the processing is a **proportionate and effective means** of achieving these purposes.

4. Balancing Test

(a) Nature of the Data

The data consists of visual images of individuals. No special category data is intentionally processed.

(b) Reasonable Expectations

Individuals would reasonably expect CCTV monitoring in locations such as workplaces and public-facing premises, particularly where signage is clearly displayed.

(c) Impact on Individuals

The impact on individuals is limited because:

- monitoring is not continuous in a live sense (passive recording);
- cameras are visible and signposted;
- private areas (e.g. toilets, changing areas) are excluded;
- access to footage is restricted and controlled.

(d) Safeguards Implemented

The RB applies the following safeguards:

- clear and visible signage informing individuals of CCTV use;
- restricted access to footage (authorised personnel only);
- retention limits (maximum 90 days unless required for investigation);
- secure storage and password protection;
- audit logging of access and disclosures;
- prohibition on covert monitoring.

(e) Vulnerable Individuals / Safeguarding Context

Where CCTV may capture vulnerable individuals, footage is handled with heightened sensitivity and access is further restricted.

5. Proportionality Assessment (DUAA-Aligned)

The RB has assessed that:

- the processing is **targeted and limited to relevant areas**;
- the benefits of the processing (safety, crime prevention) outweigh the limited intrusion;
- no less intrusive alternative would achieve the same outcomes;
- the processing is **reasonable and proportionate in the circumstances**.

6. Conclusion

The RB has concluded that:

- the processing is necessary for legitimate organisational purposes;
- it does not override the rights and freedoms of individuals;
- appropriate safeguards are in place.

Accordingly, reliance on **Legitimate Interests** is justified.

7. Review and Monitoring

This assessment will be reviewed:

- annually;
- following any significant change to CCTV use;
- following any relevant incident or complaint.

9. Approval

Approved by: Data Protection Manager at the latest Data Audit

Review Date: Next Data Audit

This assessment will be reviewed periodically and where there is a material change to the processing activity

LIA-04 – DASHCAMS

1. Processing Description

Dashcams are used in vehicles for the purpose of recording road incidents.

2. Purpose Test

- to ensure accurate recording of incidents;
- to support insurance and legal processes;
- to promote safety and accountability.

3. Necessity Test

- real-time visual recording cannot be achieved without camera technology;
- alternative methods would not provide reliable evidence.

4. Balancing Test

Nature of Data

Video footage in public spaces.

Reasonable Expectations

Individuals in public spaces have a reduced expectation of privacy.

Impact

Low, as:

- footage is not actively monitored;
- retention is limited;
- access is restricted.

Risks to individuals

The following potential risks to individuals have been identified

- loss of confidentiality;
- unauthorised access to personal data;
- misuse of personal data;
- distress or loss of privacy.

Safeguards

- limited retention;
- secure storage;

- controlled access.

5. Proportionality (DUAA)

Processing is limited to what is necessary and is proportionate to safety and evidential purposes.

6. Conclusion

The processing is justified under Legitimate Interests.

7. Approval and Review

Approved by: Data Protection Manager at the latest Data Audit

Review Date: Next Data Audit

This assessment will be reviewed periodically and where there is a material change to the processing activity