General Data Protection Regulation (2018) Policy

Context and overview

Key details

- Policy prepared by: Mick Waring
- Next review date: 7 February 2019

Introduction

Braiswick Photographic needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This also includes names and sometimes dates of birth for students and school children particularly for the production of ID cards, data matched images on CD for use in schools and named group photographs.

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 General Data Protection Regulation 2018 Policy ensures that Braiswick Photographic:

- Complies with the data protection law and follows 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

General Data Protection Regulation 2018

The General Data Protection Regulation 2018 describes how organisations — including Braiswick Photographic — 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. We are Data Protection Registered with Information Commissioners Office (ICO) registration number Z6209401.

The General Data Protection Regulation 2018 is underpinned by six important principles. These say that personal data must be:

1) Processed lawfully, fairly and in a transparent manner in relation to individuals;

2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of Braiswick Photographic
- All branches of Braiswick Photographic
- All staff and volunteers of Braiswick Photographic
- All contractors, suppliers and others working on behalf of Braiswick Photographic

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses

- Telephone numbers
- Photographs
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect Braiswick Photographic 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.

Impact Assessments

The company carries out and maintains regular Data Protection Impact Assessments on processes used within the organisation to identify and minimise the potential impact of risk within our data processing activities. Areas of the business include ID Services, Online Ordering, Sales, Photography, Accounts and Laboratory.

Responsibilities

Everyone who works for or with Braiswick Photographic has some responsibility for ensuring data is collected, stored and handled appropriately. All employees have received GDPR training.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and General Data Protection Regulation 2018 principles.

However, these people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that Braiswick Photographic meets its legal obligations.

- The **Data Protection Officer, Debbie Crees,** is responsible for:

    - Keeping the board 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 Braiswick Photographic 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.

- The **IT Director, Cam Chau,** 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.

- The **Sales Director, Mick Waring,** 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 like newspapers.
    - 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.
- Braiswick Photographic **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.
- In particular, **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 data protection officer if they are unsure about any aspect of data protection.

Data storage

Braiswick collects and uses personal data to administer orders and deliver photographs. We also use it to anticipate and resolve queries.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Director or Data Protection Officer. We do not disclose this data to any third parties.

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 are kept **in a locked drawer or filing cabinet**.
- Employees make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts are 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 is **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these are kept locked away securely when not being used. CD and DVD images are securely disposed of by use of a Data Destruction Company.
- Data is only stored on **designated drives and servers.**
- Data is **backed up frequently**. Those backups are tested regularly, in line with the company's standard backup procedures.
- Data is **never saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data are protected by **approved security software and a firewall**.
- We collect pupil information from schools for sims.net image matching, this is encrypted in a zip file before being digitally transferred to the photographers lap top to be linked with the images. This information is only requested by and provided by our employees who are DBS checked.

Data use

Personal data is of no value to Braiswick Photographic 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 ensure **the screens of their computers are always locked** when left unattended.
- Personal data **is not shared informally**.
- 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**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Supplier Agreement / Data Sharing

Suppliers that handle data on our behalf enter into a Data Sharing Agreement with Braiswick Photographic Co Ltd which includes a GDPR Supplier Questionnaire. In particular, key information on how data is processed, stored and disposed of in accordance with regulations is requested along with other assurances that GDPR requirements are being met.

Data accuracy

The law requires Braiswick Photographic 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 Braiswick Photographic 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.
- 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 Marketing Director's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Photographers

All of our photographers are DBS checked and carry a copy of their up to date certificates. Data is encrypted when transferred to their lap top for processing. Data is also encrypted once the images have been taken to be transferred to the Lab Server.

Sales Team

Our Sales Team store school contact information on company laptops within our own Customer Relation Management (CRM) system. This data includes the school name, address, telephone number and often the generic school email address. They may also collect a contact name and email address but no other personal details are stored or collected. These devices are not used for blanket coverage prospecting emails.

The laptops used are password protected and backed up to the company servicer on a regular basis. The database is password protected and can only be accessed through the company CRM application. If the database is copied it can only be accessed on a device which has the company CRM application installed and this is controlled by the I.T Director.

All of the Sales Team are DBS checked.

I.D Department

Data is stored on password protected computers in a room with key pad entry within the alarmed main building. Any paper documents and CD's containing images are stored in lockable cabinets in a key pad entry controlled room. Entry is restricted to departmental staff only who are all DBS checked.

Pre-printed cards that have the variable details added by ourselves are kept in a key pad entry controlled room.

Card design and data input is carried out using secure Positiv ID software. Data entered, if copied, can only be viewed on a device with this software installed.

Data stored for ID cards usually includes the person's name and job title where appropriate, their school / company / organisation name and sometimes a DBS registration number, if applicable. If the card is used for Proof of Age, the date of birth and sometimes an expiry date are included.

Data is stored for varying lengths of time depending on the terms of the contract or the customer's preference for the purpose of replacement or re-issue of lost or expired cards but never longer than deemed necessary. Paper copies, where held, are kept in line with

standard accounting procedures to assist in dealing with any queries that may arise at a later date.

Office and Laboratory

Only authorised employees have access to personal data. Files are kept in locked filing cabinets. Computers are password protected. Any printouts are shredded when no longer required.

We have a key pad entry system to our lab which is located in our secure head office, where all of the images are produced internally and then packed by our own internal packing department within the same building. We have alarm control and also have a separate key pad entry system to sensitive areas of the building. Key code entry is monitored by ADT Redcare Alarm Systems. We also have internal and external CCTV.

Online Orders

Braiswick online photograph orders have a bespoke system provided by our internal IT Department. All parts of the system hardware and software are owned by Braiswick Photographic Co Ltd and are not outsourced in any form. Every image is stored securely on an enclosed password protected network.

Our online orders can only be accessed with a unique username and password. Passwords are randomly generated with letters and numbers in lower and upper case with 8 characters. This gives 218340105584896 combinations. This is authenticated by server side response which then renders the html page for customer access.

Braiswick Online orders website has a SHA-256 SSL certificate provided by Symantec Corporation (known for the Norton Antivirus) Card payments are provided by Sagepay who deal with the complete process of handling the card payments. This means that we do not process payment information and do not store it ourselves. The payment is transacted through Secure Server Software, which encrypts all of the information so that it can't be intercepted.

Orders that are sent to home addresses are not sent with any identifiable data other than name and address of the person who placed the order.

Payments

Any visa or credit card, cheque and cash payments that are handed in to the school are collected by one or our employees in a secured bag and taken directly to our secure head office. They are stored in our electronically secured safe until processed in a secure office with key pad entry system which only authorised employees have access to. Visa and credit

card slips are then stored in the safe for a period of three months when they are securely destroyed.

Servers

Our servers are all located in our secure head office premises. Our images are not stored with any cloud based software.

Storage

Data is retained for 60 days on the photographers laptop and 18 months on the company data server to assist with queries and any late orders. The data is backed up by encrypted internal data storage. Only authorised office and lab staff have access to the data.

Security

We constantly review the encryption methods and levels of our digital files that are required to be transferred. We use security software to test our network for vulnerabilities. Data is stored on a closed network with no outside connection to prevent cyber-attacks.

Wired and wireless network intrusion are tested every school term and network infrastructure is evaluated for hardware renewal.

Subject access requests

All individuals who are the subject of personal data held by Braiswick Photographic 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 requests from individuals should be made verbally or by email, addressed to the Data Controller at d.crees@braiswick.co.uk. or 01206 399800. The Data Controller can supply a standard request form, although individuals do not have to use this.

The Data Controller will provide the relevant data within 28 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 General Data Protection Regulation 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Braiswick Photographic will disclose the requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Braiswick Photographic 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 statement, setting out how data relating to individuals is used by the company.

This is available on request. A version of this statement is also available on the company's website, www.braiswick.co.uk under the FAQ section.