GENERAL DATA PROTECTION REGULATION (GDPR) STATEMENT
DSimaging Ltd GDPR Assessment 2018.

INTRODUCTION

GDPR sets out and legislates how DSimaging Ltd collects, stores and handles personal information on digital paper and any other media.
This legislation is effective from the 25th May 2018 and prior to the introduction of the said legislation.
DSimaging is fully supportive and subscribed to the outgoing Data Protection Act.
Eventure Photography / Eventure School Photography and Pics4Paws will hereafter be referred to as DSimaging Ltd.

For further information see the ICO website and GDPR information at https://ico.org.uk/

ASSESSMENT

DSimaging Ltd conducted a GDPR assessment and has determined that DSimaging Ltd obtains and processes data in the following way:

1. A data and controller and processor of third party data.
2. A data controller and processor of data, for example activity relating to direct marketing For school services and customers, including photography and marketing services.

DSimaging Ltd works with the following data:

- Customers
- General Business Contacts
- Suppliers

This can also include other businesses or individuals. These are categorised as **A**. Consent
B. Legitimate Business interest.

DSimaging Ltd subscribe to the GDPR regulations and by doing so we ensure that we maintain the following:

- Comply with the data protection law and follow good practice.
- Protect the rights of customers and partners.
- DSimaging Ltd are open about how it stores and uses individuals' data.
- DSimaging Ltd protects itself against risk of data breach.

By doing so, we ensure that we adhere to the six principles of GDPR as detailed under Article 5 as shown below:.

1. Personal information shall be processed lawfully, fairly and in a transparent manner.

Jargon deciphered, principle one specifically points toward the concept of clear consent. In any situation where personal information is collected, it should have the demonstrable consent of the data subject. Opt-in tick boxes are still permitted, but the regulation explicitly prohibits consent by non-action or opt-out boxes. The death of those confusing subscription choices at the bottom of forms is on the horizon.

2. Personal information shall be collected for specified, explicit and legitimate purposes.

Where personal information is collected, it must be communicated to the data subject, the purpose for its collection and subsequent processing. Organisations are going to need to become much clearer with data subjects about what their personal information is going to be used for.

3. Personal information shall be adequate, relevant, and limited to what is necessary.

When collecting personal information, the data controller must only collect personal information that is absolutely required for the specified purpose. For example, if collecting personal information to send a magazine subscription, there is no basis for the requirement of my date of birth.

4. Personal information shall be accurate and, where necessary, kept up-to-date.

It is now the obligation of the data controller to ensure – to the best of their abilities – that the information collected is correct. This may seem difficult and even trivial; however, what the regulation is trying to address are situations where processing incorrect personal information may cause distress or harm to data subjects.

5. Personal information shall be retained only for as long as necessary.

Marketing teams wince at this principle as though it is the sourest of grapes on the vine. All personal information must now have an expiration date applied appropriate to its collected purpose. Indefinite retention is unlikely to ever entertain the patience of the supervisory authority.

6. Personal information shall be processed in an appropriate manner to maintain security.

The principle that has attracted much focus, for it requires data controllers and processors to ensure that their systems maintain the confidentiality, integrity and availability of data processing systems.

Article 5 of the GDPR sets out the six principles of data protection. These principles are the Foundation of the GDPR and require that is:

A. “Processed lawfully, fairly and in a transparent manner in relation to individuals.
B. Collected for specific, 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.
C. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
D. Accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed are erased or rectified without delay.
E. Kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed for soley for archiving purposes in the public interest, scientific or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the individual: and
F. 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 and technical or organisational measures.”

http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-dpr/principles/

DSimaging Ltd Responsibilities Under GDPR

DSimaging Ltd GDPR statement applies to the following:

- The registered head office of DSimaging Ltd.
- Any individual or supplier working for DSimaging Ltd on instruction.

Dsimaging Ltd GDPR statement covers the following data we process - where an individual can be identified from the said data:

- Names
- Email addresses
- Postal addresses
- Telephone numbers
- Details required to process payments
- Photographs
- Any other data which could be required to identify an individual

Responsibilities

DSimaging Ltd has a requirement to ensure data is collected, stored and handled appropriately.

Any person or persons actively involved with DSimaging Ltd are required to adhere to the General Data Protection Regulation 2018 principals.

The Board of Directors are responsible for ensuring that DSimaging Ltd meets it's legal obligations.

The Data Protection Officers (DPO's) are **David Shortland** and **Chantelle Shortland**
ie: 'The Directors'

- Reviewing all data protection procedures, in line with the agreed schedule.
- Dealing with requests from individuals to see the data DSimaging Ltd 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.
- 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.
- Approving any data protection statements attached to communications such as emails and letters.
- Evaluating any third-party services the Company is considering using to store or process data, for example cloud computing services.
- Addressing any data protection queries from journalists or media outlets, for example newspapers.
- Where necessary, ensuring marketing initiatives abide by data protection principles.

DSimaging Ltd Guidelines

- The only people able to access data covered by this policy shall be those who need it for their work.
- Data will not be shared informally.
- All data will be held securely by taking sensible and reasonable precautions and following the guidelines below.
- Robust passwords must be used and never shared.
- 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. If physical data, it should be shredded.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to officers of the Company. DSimaging Ltd uses personal data to allow ordering, management and delivery of our photographic and marketing services.

- When not required, the paper or files are kept in a locked drawer or cupboard.
- Printouts and documents are not left on show where unauthorised people could see them ie: 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 using appropriate digital security.
- Data is protected by strong passwords that are changed regularly and never shared.
- If data is stored on a removable media (eg: CD or DVD), these are locked away securely when not being used. CD and DVD images are securely disposed of when finished with.
- Data is only stored on designated drives and servers within the UK.
- Laptops are never left in vehicles overnight or left unattended.
- Data is backed up frequently. Those backups are tested regularly in line with our standard backup procedures.
- Data is never saved directly to mobile devices eg: tablets or smartphones.
- All servers and computers containing data are protected by approved security measures.

Data Use

- When working with personal data, computer screens are always locked when unattended.
- Personal data is not shared unnecessarily.
- Sensitive data must be protected before being sent electronically **(Unidentifiable photographs are not classed as sensitive data).**
- Personal data is not transferred outside of the European Economic Area.
- DSimaging Ltd does not share data with third parties.
- Personal data will only be stored on designated computers.

Data Accuracy

The law requires that DSimaging takes all 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 DSimaging Ltd should put into ensuring the datas accuracy.

It is the responsibility of all who work with data to take reasonable steps to ensure it is kept up to date and as accurate as possible.

- Data will be held in as few places as necessary and unnecessary data sets will not be created.
- Data should be updated at every opportunity ie: 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.

Photographers

Laptops are encrypted and secure password protected. Images on laptops are encrypted.Photographers are DBS checked which is available on request.

Security

Security is subject to ongoing review across both digital and physical security.

Subject Access Request (SAR)

All individuals who are the subject of personal data held by DSimaging Ltd are entitled to:

- Ask what information is held about them by the company.
- Ask how to gain access to the said data.
- Be informed how it is kept up to date.
- Be informed how the company is meeting its GDPR obligations.

If an individual contacts the company requesting this information, this is called a **Subject Access Request** or **(SAR)**.

Subject access requests from any individual or business should be made by email to **info@dsimaging.co.uk**.

The designated person will aim to provide the information within 28 days.
The identification of anyone making such a request will be verified before handing over the information.

DSimaging Ltd will delete the information on request by the individual or business in its entirety.

DSimaging Ltd does not charge for subject access requests.

Disclosing Data for other reasons

In certain circumstances the GDPR regulation 2018 allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, DSimaging Ltd will disclose the requested data.
However, the Directors will ensure the request is legitimate, seeking legal advice where necessary.
DSimaging Ltd aims to ensure that individuals are aware their data is being processed and that they understand:

- How the data is being used.
- How to exercise their rights under GDPR.

Head Office and Processing

Our office is not accessible by the general public. Computers are password protected.
Physical data is shredded once finished with.

All DSimaging Ltd images are produced by a GDPR compliant photographic laboratory and packed by our own internal department. Final images are hand delivered wherever possible with no identifying data other than the recipients name and address.

Customer Orders

Every image is stored securely on a firewall protected network. Customers can also order by post, telephone or email or in the case of school photo proofs through a back to school process where parents return the orders via the school.
Where appropriate, customers can only access online ordering through secure a secure photo code provided to them to access their images. Photographs cannot be accessed without a unique code.

DSimaging Ltd uses secure trading through PayPal and is PCI compliant.
PayPal handle all card payments. Once the transactions are completed no data is held either electronically or physically.
In addition to card payments, payments can also be made by cash and cheque and once these are processed, details are then destroyed.
All orders made through a school will be fulfilled within 10 working days of receipt of orders. Customers then have 7 days to query any discrepancy in payment once their order is received, whereupon a refund or replacement product will be offered where and if appropriate.

Data Storage

Data is stored for as long as deemed necessary for the relevant job.
Photographs are stored for varying lengths of time depending on usage. Images can be stored for up to ten years as DSimaging Ltd finds that in the case of school photography, parents often purchase older photographs when they have forgotten to order at the time, or to purchase images of their child when they were younger. Often schools ask for previous year group headshots for their records.

Regarding schools contact information this is refreshed against the Department of Education's most recent school listing or when we identify a change through normal day to day business operations.