EMILY PB
FINE ART & ANTIQUES CONSULTANT

Data Protection Policy

v.2

Key details

EMILYPB, FINE ART & ANTIQUES CONSULTANT

Mansfield House, Strathmiglo, Cupar, Fife KY14 7QE

- Policy prepared by: Emily Pelham Burn
- Version Number: v.2.
- Approved by management on: 19/08/2022
- Policy became operational on: 19/08/2022

Introduction

EMILYPB needs to gather and use certain information about individuals both as a Data Controller and Processor. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. 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 data protection policy ensures EMILYPB:

- Complies with 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.

Data Protection Law

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) (GDPR 2018) describes how organisations, including EMILYPB, 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 data must be processed lawfully, stored safely and not disclosed unlawfully.

The GDPR is underpinned by eight important principles. These say that personal data must:

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
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities

Policy scope

This policy applies to:

- The office of EMILYPB
- All staff of EMILYPB
- All contractors, suppliers and other people working on behalf of EMILYPB. It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR.

This can include:

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

- …plus any other relevant data relating to individuals such as photographs or lists of art or other house contents which are potentially identifiable.

Will EMILYPB share my personal data with anyone else?

We may pass your personal data on to third-party service providers contracted to EMILYPB in the course of dealing with you. Any third parties that we may share your data with are obliged to keep your details securely, and to use them only to fulfil the service they provide you on your behalf. When they no longer need your data to fulfil this service, they will dispose of the details in line with EMILYPB's procedures. If we wish to pass your sensitive personal data onto a third party we will only do so once we have obtained your consent, unless we are legally required to do otherwise.

Data protection risks

This policy helps to protect EMILYPB 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 EMILYPB has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone handling personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- **Emily Pelham Burn** is ultimately responsible for ensuring that EMILYPB meets its legal obligations.

- **Emily Pelham Burn** is responsible for:
  - Keeping EMILYPB updated about data protection responsibilities, risks and issues;
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule;
  - Ensuring the parties covered by this policy have received relevant data protection training or advice;
  - Handling data protection questions from staff and anyone else covered by this policy;
  - Dealing with requests from individuals to see the data EMILYPB 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 manager, Emily Pelham Burn**, 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 Marketing Manager, Emily Pelham Burn**, 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**.
- EMILYPB **will provide training** to all employees and authorised third parties, where necessary, 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 Emily Pelham Burn 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 data controller.

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 the office or securely shredded**.
- Employees should make sure paper and printouts **are not left where unauthorised people could see them**.
- **Data printouts should be shredded** 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 regularly and never shared between employees.
- If data is **stored on removable media** (like a USB disk or thumb drive), these media should be first encrypted using Microsoft BitLocker encryption. CDs and DVDs are no longer used for this purpose.
- Data will only be stored on **designated drives and servers**, and will only be uploaded to an **approved cloud computing service**.
- Servers containing personal data are **sited in a secure location**.
- Data is **backed up frequently**. These backups tested regularly, in line with the company's standard backup procedures. These backups are encrypted using Microsoft Bitlocker Encryption.
- Data will **never be saved directly** to laptops or other mobile devices like tablets or smart phones which are either unauthorised or unencrypted.
- All servers and computers containing data are protected by **approved security software and a firewall**.
- All PCs, laptops, USB disks and USB Thumb drives used to store personal information are encrypted using Microsoft Bitlocker Encryption.

Data use

- Personal data is of no value to EMILYPB 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, therefore:
- 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 insecure email channels.
- Data should be only be **transferred electronically across encrypted connections** and to cloud storage that is encrypted 'at rest'. The IT manager can explain

how to send data to authorised external contacts or destinations. Examples of encrypted connections used by EMILYPB include but are not limited to:
    - SharePoint file sharing;
    - DropBox file sharing;
    - Email sent over end-to-end encrypted connections such as Microsoft 365 email using the Outlook App;
    - Other reputable GDPR-compliant file transfer companies such as WeTransfer.
- Personal data will **never be transferred outside of the European Economic Area**.
- Employees **are prohibited from saving copies of personal data to their own devices**, unless expressly authorised in writing by the IT Manager.

Data accuracy

The law requires EMILYPB 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 EMILYPB 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.
- EMILYPB will make it **easy for data subjects to update the information** EMILYPB holds about them.
- 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 EMILYPB 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 by email, addressed to the data controller at info@emilypb.co.uk
- Individuals will be charged £10 per subject access request only if an unreasonable number of requests are deemed to have been requested.
- The data controller will aim to provide the relevant data within 1 month of receiving your request and verifying your identity unless such data is restricted by law. Verification will require the supply of appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address).
- 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 GDPR 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, EMILYPB will disclose requested data. However, the data controller will ensure the request is

legitimate, seeking assistance from the company's legal advisers where necessary.

Providing information

EMILYPB 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.

EMILYPB's Privacy Policy is available on request by contacting Emily Pelham Burn by email at info@emilypb.co.uk and is also available on the company's website – www.emilypb.co.uk