GDPR Data Protection Policy

Key details

Policy revision control:	Version 1.1
Policy prepared by:	Chris Oxlade-Arnott
Approved by business owners on:	7th January 2019
Policy became operational on:	7th January 2019
Next Review date:	6th January 2020

Induction

Participate In Art (PIA) - also known as pARTicpate, 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 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 PIA:

- Complies with data protection law and follow good practice
- Protects the rights of employees, 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) May 2018 describes how organisations, including Architectural Impressions UK, must collect, handle and store personal information.

These regulations 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.

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/workplace of PIA
- All/any employees and volunteers of PIA
- All/any contractors, suppliers and other people working on directly behalf of PIA.

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

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Social media contacts
- Any other information relating to individuals.

Data protection risks

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

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

These people have key areas of responsibility:

The Company Owners are ultimately responsible for ensuring that PIA meets its legal obligations.

The Data Protection Officer – Mr Chris Oxlade-Arnott, is responsible for:

- Keeping the company owners 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 employees and anyone else covered by this policy
- Dealing with requests from individuals to see the data PIA 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 Authority – Mr Chris Oxlade-Arnott, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable and proportionate 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 Authority – Mrs Jilly Oxlade-Arnott, 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 such as newspapers
- Where necessary, working with other employees to ensure marketing initiatives abide by data protection principles.

General Employee 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 managers
- PIA 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 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 manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These regulations describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Authority or Data Protection Officer (in this case is the same individual).

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 normally stored electronically but has been printed out in hard copy:

- When not required, the paper or files should be kept in lockable filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them, such as, on a printer
- Data printouts should 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 regularly and never shared between employees
- If data is stored on removable media (such as, a CD/DVD or memory drive), these should be kept locked away securely when not in use
- Data should only be stored on designated drives and servers, and should only be uploaded to the company approved cloud computing services
- Data should be backed up regularly. Those backups should be tested frequently, in line with the company's standard backup procedures (if available)
- Data should never be saved directly to laptops or other mobile devices, such as, tablets or smart phones
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to PIA unless the business can make use of it. However, when personal data is accessed and used it is at this point where the greatest risk of loss, corruption or theft may occur:

- 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 email, as this form of communication is not secure
- Data must be encrypted before being transferred electronically. The IT Authority 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.

Data accuracy

The law requires PIA to take reasonable steps to ensure data is kept accurate and up to date.

It is essential that personal data is accurate.

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. Employees should not create any unnecessary additional data sets
- Employees should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call
- PIA will make it easy for data subjects to update the information PIA holds about them. Such as, via the company website
- Data should be updated as inaccuracies are discovered. Such as, if a customer can no longer be reached on their stored telephone number, it should be removed from the database
- It is the Marketing Authority's responsibility to ensure marketing databases are checked against industry suppression files annually.

Subject access requests

All individuals who are the subject of personal data held by PIA 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 Protection Officer (DPO) – Mr Chris Oxlade-Arnott. The DPO can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £25.00 per subject access request. The DPO will aim to provide the relevant data within 14 days of the request and payment.

The DPO 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, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, PIA will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the Owners and from legal advisers where necessary.

Providing information

PIA 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 website.