

Data Protection Policy (GDPR)

Kingfisher Press LTD

May 2018

Prepared by: Nina Tomlin

Date: 01/05/2018

1. Introduction
2. Responsibilities
3. Confidentiality
4. Security
5. Data Recording and Storage
6. Subject Access
7. Transparency
8. Consent
9. Direct Marketing
10. Staff Training
11. Policy Review
12. Privacy Statement - Website

Introduction

Purpose of Policy

To comply with the current GDPR and Data Protection Regulations. To follow good practice in protecting clients, staff, suppliers and prospects and to protect the organisation.

Data Protection Principles

Specifically, the Principles require that personal information:

- a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
- b) Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
- c) Shall be adequate, relevant and not excessive in relation to those purpose(s)
- d) Shall be accurate and, where necessary, kept up to date,
- e) Shall not be kept for longer than is necessary
- f) Shall be processed in accordance with the rights of data subjects under the Act,
- g) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- h) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

Personal Data

Personal data is any data which relates to an identifiable living individual.

Policy Statement

Kingfisher Press Ltd will comply with the GDPR rules and regulations on managing personal data including personnel, clients, suppliers and prospects for marketing purposes.

All files are stored in a secure and password protected location.

Staff will be trained in the management of handling personal data.

Any requests for data held on an individual employee, prospect or a client can be viewed upon approved request by that individual. No company or financial information can be viewed, only 'personal' data on the requesting individual.

Document Scope

This document covers the management of data at Kingfisher Press Ltd.

It applies to all the data the company holds for marketing purposes that relate to identifiable individuals.

This can include:

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

Data Protection Risks

- Breaches of confidentiality – information being given out inappropriately
- Failing to offer choice – asking if ok to keep data for marketing purposes

Responsibilities

Everyone who works with marketing data at each Kingfisher Press Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

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

The board of directors is ultimately responsible for ensuring that the company meets its legal obligations.

Directors are responsible for:

- Keeping the board updated on data protection responsibilities
- Reviewing data protection procedures and policies
- Arranging training and advice for staff
- Handling questions and enquiries from staff
- Dealing with requests from individuals to the data Kingfisher Press Ltd holds about them (Subject access request)
- Checking and approving any agreements with third parties who may handle sensitive data
- IT – ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Evaluating third party services – ie cloud services.

The Marketing Manager is responsible for:

- Working with marketing staff to ensure marketing initiatives abide by data protection
- Ensuring Marketing Prospect Data is stored and managed correctly

Enforcement

All personnel who do not comply with the Data Protection Policies will be subject to disciplinary procedures.

Confidentiality

Scope

All information held within Kingfisher Press is classed as confidential.

All data is treated as confidential. Access to personnel data, financial, sales and marketing data is restricted to relevant staff only.

This covers all departments including:

- HR
- Sales & Marketing
- Accounts & Finance
- Warehouse & factory
- Data protection approval for 3rd party suppliers

Communication with Staff

This data protection policy will be communicated to all staff to ensure they are aware and understand the rules of data protection.

Security

Scope

Security of all data held by Kingfisher Press Ltd. All data held by the company for the purposes of business.

Security Measures

All systems are password protected.

Files held on the secure server are locked down with access to relevant staff members.

Accounts and financial data is accessed via a restricted secure log in.

Private personnel files are stored in a secure folder. Physical files in a locked safe.

Business Continuity

All data is backed up – any breach in security should be reported immediately to a Director.

Specific Risks

- Breaches of confidentiality – information being given out inappropriately
- Failing to offer choice – asking if ok to keep data for marketing purposes

Data Recording & Storage

Data Accuracy

The law requires Kingfisher Press Ltd takes reasonable steps to ensure the data is kept accurate and up to date.

- Data will be kept in as fewer places as necessary
- Staff should take every opportunity to update data
- It is the responsibility of the marketing manager to ensure that marketing databases are checked against industry suppression files every six months.

Updating

Prospect data will be accurate and kept up to date when necessary by regular contact.

Clients will be updated on a regular basis by way of a working relationship.

Personnel files are reviewed annual and any changes updated as they happen.

Storage

Stored on paper

- Paper and printouts should not be left where un-authorized people can see them.
- Data printouts should be shredded and disposed of securely.

Stored Electronically

- Data should be protected by strong passwords that are changed regularly
- Any removable media should be locked away or stored securely
- Data must be stored on designated drives and approved cloud computing
- Backed up frequently
- Data will not be saved directly to laptops or other devices.
- All servers have approved security software and firewall.

Data Use

- Ensure screens are locked when un attended
- Data should not be shared informally
- Personal Data must be encrypted before being transferred electronically
- No personal data or artwork containing personal data will be sent/received via email.
- Personal data should never be transferred out of the European Economic Area
- No personal data should be saved to any personal computer.

Retention Periods

Old/not current clients remain on the accounting system indefinitely with minimal data/info.

Cold prospects are kept on a suppression list with minimal data retained indefinitely.

Direct Mail data is deleted up completion of the project.

Personalised project data will be deleted up project completion.

Artwork containing personal information will only be retained following approval from the client. If no approval is given it will be deleted when the project is complete.

Archiving

Old Data is stored on the server in a secure file – only to be accessed for archived research purposes.

Email data is kept in an archived to secure file.

Client personal data supplied for direct mail is deleted.

Non-personal artwork is retained on a secure server with password protection and limited access.

Subject Access

All individuals who are subject to the personal data held by Kingfisher Press Ltd are entitled to:

- Ask what information is held 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 data protection obligations

Procedure for making a request

Requests must be made in writing and only by the data subject allowing basic information to be shared regarding that individual only to a director.

Proof of identity will be required before any data is handed over.

Procedure for granting access

Any physical information will be printed and handed to the data subject. Any digital data can be viewed by the data subject while overseen by the data control officer.

Transparency

Commitment

Data held by Kingfisher Press is for the purposes of offering a business to business transaction, either client, supplier or prospect.

Prospect information is held in order to engage new business. Any prospect can request to see the data Kingfisher holds on them at any time.

No data is shared with any other organisation – unless specifically requested as part of the order by the client.

Personnel data for the purpose of employment and health and safety is kept in a secure manner.

Consent

Underlying Principles

No data will be held unless Kingfisher has a good reason.

To ensure all electronic communications have permission by the data subject.

Postal campaigns will only be sent to those not on the MPS list.

Any company listed on the CTPS/TPS register will not be contacted by telephone.

Forms of Consent

All new prospects are requested to approve continued contact for marketing purposes in the form of an email which is kept to provide an audit trail for consent.

All client/supplier data is kept with consent of the data subject by means of an on-going business relationship.

Any data supplied by a client is the responsibility of the client, not Kingfisher Press Ltd.

All marketing prospects must give consent in order to receive Kingfisher Press e-marketing information.

Verbal consent will be noted on the prospect details held by the account manager.

Opting Out

All prospects and clients have the opportunity to opt-out of communications on e-marketing campaigns.

Withdrawing Consent

Prospects / clients have the right to withdraw consent. Records have to be kept for a period of time – to ensure we do not contact them again.

Direct Marketing

Underlying Principles

To ensure all electronic communications have permission by the data subject. To ensure any data held by Kingfisher Press is managed and controlled correctly.

Opting Out

All electronic communications have an opt-out option which is either part of the e-marketing campaign or administered manually by each Sales Team Member.

Sharing Lists

Mail Sort / Direct Mail Data: Company providing outsourced services must have Data Protection / privacy policy in place. We do not send any electronic campaigns on behalf of clients.

Data Management procedures available in the Kingfisher Press Ltd Policy and Procedures Manual regarding Direct Mail outsourced projects.

Electronic Contact

All prospects will be asked if they wish to receive electronic communications going forward.

Emails will be kept as a point of reference.

Staff Training

Documentation

This document will be available to all staff. All staff will be required to read and sign a consent of notice form.

Related Policies

Other related policies:

- Sales & Marketing Procedures
- Data Management
- Staff Handbook
- Policies and Procedures Manual

Induction

All staff will receive Induction training on this policy when they join Kingfisher Press.

Continuing Training

Quarterly sales meeting review will include review of data

Annual appraisals will include any updates to this policy.

IT review including data management review will be conducted as any new developments arise.

Procedure for Staff Signifying Acceptance of Policy

All office staff and factory will be required to read this policy and sign a consent of notice form.

Policy Review

Responsibility

This policy will be reviewed in 2021 by the Directors.

Procedure

The data control and management procedures will be reviewed and updated where necessary.

All staff will be required to read and understand the updated policy.

Timing

The review will begin in October 2020 in order to be completed by April 2021.

Privacy Statement - Website

Data collection

Personal data

All personal data is collected and stored in line with the Data Protection Act 1998.

We collect the following data:

- Click-stream data (the type of computer and browsing software you use, the address of the web site from which you linked, etc)
- HTTP protocol elements (your server address and top level domain name (eg .com, .gov etc), date and time of visit, etc)
- Search terms

This data will be used for the following purposes:

- Completion and support of the current activity.
- Web site and system administration.
- Research and development.

This data is collected from all web users. Web access logs are used for statistical purposes only (eg to measure the use/performance of the site) except in the event of a security breach when they could be used for the purpose of tracing the breach. No information gathered from web logs is given or sold to any third party.

Any personal information that you provide to us will only be used for the purpose stated at the time we request it. This information will not be disclosed to a third party except where authorised by you or as otherwise permitted by the Data Protection Act.

Cookies

Cookies are a technology which can be used to provide you with tailored information from a web site; they can facilitate communication and interaction with the site. You may stop or restrict the placement of cookies on your computer by adjusting your web browser preferences, but this may interfere with some of the functionality of the site.

Cookies will be used for the following purposes:

- Research and development.
- User targeting.
- This data will be used by ourselves and our agents.

Cookies are used to track visitors to our site.

E-mail and electronic forms

We collect the following information:

- Physical contact information
- Online contact information
- Preference data

This data will be used for the following purposes:

- Completion and support of the current activity.
- Contacting visitors for marketing of services or products.

In all cases this information will only be used for the stated purpose for which it was provided. A number of online forms are provided on this site. Each form is processed using standard mail techniques, and is not encrypted.

The data is collected so that we can send you news and other information which is relevant to your needs and interests.