KINGDOM
Group

Privacy Policy

If you need this publication in larger print, audio form, Braille, or in another language, please contact our office and we will try to help you.

HAPPY TO TRANSLATE

Approved: May 2018
Next Review: May 2023

Privacy Policy

1. Introduction

The Kingdom Group (Kingdom) is committed to ensuring the secure and safe management of data in relation to our customers, staff and other individuals. Our staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with this policy.

Kingdom needs to gather and use certain information about individuals. Kingdom manages a significant amount of data, from a variety of sources across the Group structure. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

It is a legal requirement that Kingdom process data correctly; we must collect, handle and store personal information in accordance with the relevant legislation.

2. Data

Kingdom holds a variety of Data relating to individuals, including customers and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by us is detailed within the Fair Processing Notice.

"Personal Data" is that from which a living individual can be identified either by that data alone or in conjunction with other data held by Kingdom.

Kingdom also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

3. Processing of Personal Data

Kingdom is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject;
- Processing is necessary for the performance of a contract between Kingdom and the data subject or for entering into a contract with the data subject;
- Processing is necessary for Kingdom's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of Kingdom's official authority; or
- Processing is necessary for the purposes of legitimate interests.

Fair Processing Notice

Kingdom has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held.

The Fair Processing Notice sets out the Personal Data processed by Kingdom and the basis for that Processing.

Employees

Details of the data held and processing of that data is contained within the Employee Fair Processing Notice. A copy of any employee's Personal Data held by us is available upon written request by that employee from Corporate Support Services, Service Coordinator or Data Protection Officer.

Consent

Consent as a ground of processing will be used from time to time when processing Personal Data; it will only be used by us where no other alternative ground for processing is available.

Processing of Special Category Personal Data or Sensitive Personal Data

In the event that we process Special Category Personal Data or Sensitive Personal Data, we will do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

4. Data Sharing

Kingdom shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with our relevant policies and procedures. To monitor compliance by these third parties with Data Protection laws, we require the third party organisations to enter in to an Agreement with us governing the processing of data, security measures to be implemented and responsibility for breaches.

Data Sharing

Personal data is from time to time shared amongst Kingdom and third parties who require to process personal data that Kingdom process as well. Both us and the third party will be processing that data in their individual capacities as data controllers.

Where Kingdom shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement.

A data processor is a third party entity that processes personal data on behalf of the us, and are frequently engaged if certain of Kingdom's work is outsourced (e.g. maintenance and repair works). A data processor must comply with Data Protection laws.

Where we contract with a third party to process personal data held by us, we require the third party to enter in to a Data Protection Addendum.

5. Data Storage and Security

All Personal Data held by us will be stored securely, whether electronically or in paper format.

Paper and Electronic Storage

Personal Data stored on paper and/or electronically will be kept in a secure place where unauthorised personnel cannot access it with a retention schedule in place for its destruction.

6. Breaches

A data breach can occur at any point when handling Personal Data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally to the Information Commissioner's Office (ICO) within 72 hours of the breach occurring.

7. Data Protection Officer (DPO)

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance with Data Protection laws. Kingdom has elected to appoint Calum Kippen, Governance Manager as the Data Protection Officer. His details are noted on our website and contained within the Fair Processing Notice.

8. Data Subject Rights

Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by us, whether in written or electronic form.

Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to Kingdom's processing of their data. These rights are notified in the Kingdom's Fair Processing Notice.

Subject Access Requests

Data Subjects are permitted to view their data upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, we will respond to the Subject Access Request within one month of the date of receipt of the request.

.

The Right to be Forgotten

A data subject can exercise their right to be forgotten by submitting a request in writing to the DPO seeking that we erase the data subject's Personal Data in its entirety.

Each request received by our DPO will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request and will respond in writing to the request.

The Right to Restrict or Object to Processing

A data subject may request that we restrict our processing of the data subject's Personal Data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by us, a data subject has an absolute right to object to processing of this nature, and if we receive a written request to cease processing for this purpose, then we will do so.

Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request and will respond in writing to the request.

9. Privacy Impact Assessments (PIAs)

These are a means of assisting us in identifying and reducing the risks that our operations have on personal privacy of data subjects. We will carry out a PIA before undertaking a project or processing activity which poses a “high risk” to an individual’s privacy.

10. Archiving, Retention and Destruction of Data

We will not retain Personal Data indefinitely; we will ensure that Personal data is only retained for the period necessary.

Privacy Policy

Reference made to the following legislation, sources and other guidance:

(a)the General Data Protection Regulation (EU) 2016/679 ("the GDPR");
(b)the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
(c)any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.
(d) SFHA model policy
(e) ICO GDPR Guidance
(f) Addleshaw Goddard Data Protection report on the Kingdom Group

Prepared by: Calum Kippen, Data Protection Officer and Governance Manager

Draft 1 Reviewed by Data Protection Working Group

Presented to Board of Management on 21st May 2018

Policy Approved: May 2018

Next review date: May 2023