Data Protection Standard

Version:	V.02
Approved on:	12 November 2019
Original approval:	9 January 2018 by Karen Witts, CFO and Alastair Robertson, CPO
Owner:	Group Data Protection Officer
Next Update due:	December 2020

1. Summary and objective(s)

The purpose of this Standard is to ensure compliance with data protection and privacy laws and to ensure the data of our customers, employees and suppliers is always collected and used appropriately in any jurisdiction in which Kingfisher Group Companies operate.

In this Policy Standard, "**Personal Data**" means information which, taken individually or in combination with other information, allows the identification of a person ("**Individual**"). This includes, for example: the professional email address of an Individual, his/her first name in conjunction with postal address or date of birth, a photograph of an Individual etc…

Personal Data must be kept secure and be treated fairly, transparently and in accordance with the law at all times.

Each Group Company must be aware of the regulatory framework applicable to the territories in which it operates.

- Within the European Union, the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is applicable from 25 May 2018, along with other privacy-related laws or local data protection rules;
- Outside the European Union, any local or regional laws applicable to the Group Company's activities must be complied with.

The Group Data Protection Officer will establish and enforce effective compliance procedures with the support of the person who, within each country in which Kingfisher operates, has responsibility for data protection questions ("**Data Protection Leads**").

2. Accountability and governance

2.1 THE GROUP DATA PROTECTION OFFICER is responsible for this Policy Standard and its implementation throughout the Group.

The role and responsibilities of the Data Protection Officer are as follows:

- keeping the Board of Directors updated about data protection responsibilities, risks and issues;
- reviewing and approving all data protection procedures and policies on a regular basis;
- monitoring compliance with the procedures, policies and the applicable data protection and privacy laws;
- arranging data protection training and advice for all staff members and those included in this policy;
- answering questions on data protection from staff, board members and other stakeholders;

- responding to individuals such as customers and employees who wish to know which data is being held on them and checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing;
- overseeing and reviewing privacy impact assessments;
- being a point of contact to the lead supervisory authority and cooperating with the local supervisory authorities.

The Data Protection Officer can be contacted at dpo@kingfisher.com

Please note that all the Kingfisher companies and all functions within the Group are required to disclose, without undue delay, any information the Data Protection Officer may reasonably need in order to fulfil his/her role.

2.2 THE DATA PROTECTION LEAD is in charge of:

- helping the Data Protection Officer understand local legislation regarding privacy and Data Protection law;
- helping the Data Protection Officer define data protection rules and processes in a country or territory in which Kingfisher Group Companies operate;
- being a link between the Data Protection Officer and the relevant Kingfisher Group Companies in a country in relation to data protection and privacy matters.

A list of Data Protection Leads is available here: **https://www.kingfisher.com/content/dam/kingfisher/Corporate/Documents/code-of-conduct/Data_Protection_Team.pdf**

2.3 The IT GOVERNANCE TEAM is responsible for ensuring data security on Kingfisher and third-party systems.

The IT Governance team should always be consulted in the event data is processed by a Group Company or a third party. The points of contact within the IT Governance team are detailed on the Intranet and updates will be regularly communicated by Internal Communications.

Role and responsibilities of the IT Governance Team:

- ensure all systems, services, software and equipment meet acceptable security standards;
- ensure all systems, services, software and equipment allow compliance with data protection policies, standards, process, guidelines and the laws of the relevant countries;
- drafting systems and information security policies and contract documents;
- conducting third-party due diligence.

3. Group Minimum standards

Unless the applicable laws of a jurisdiction in which Kingfisher Group Companies operate impose more stringent requirements (in which case, those more stringent requirements will apply), the following standards should, at all times, be complied with throughout the Kingfisher Group when handling the Personal Data of employees, customers and suppliers. More detailed and country-specific rules will be communicated to each Kingfisher Group Company by the Data Protection Officer or the Data Protection Lead.

3.1 Data collection:

Prior to collecting Personal Data:

- we must ensure that we collect only the minimum Personal Data necessary for the purpose;
- we must ensure that the purpose of collection is legitimate and not in violation of the Individuals' rights;
- we must inform the Individuals, in a clear manner, of the use we intend to make of their Personal Data and the reasons for the collection;
- we must ensure the Persona Data will be collected and stored in a safe manner and that adequate security measures are in place to prevent unauthorised access, damage or loss to the Personal Data.

3.2 Data handling:

- we must ensure that the Personal Data is not available to people who do not need to have access to it;
- we must ensure that Personal Data is only used for the purposes for which it was collected and as would be reasonably expected by the Individual to which it relates;
- we must regularly check and confirm that the data is handled and stored in a safe manner and is protected from unauthorised access, damage or loss;
- we must identify and always record in a format to be communicated by the Data Protection Officer, the following information: (i) categories of data collected and handled, (ii) categories of Individuals whose data will be processed, (iii) categories of recipients to whom the Personal Data have been or will be disclosed, (iv) address of the location(s) the data is stored.
- The Data Protection Officer or the Data Protection Lead should always be contacted prior to using any automated processing tool resulting in automated decisions being taken about an Individual, i.e. evaluating certain personal aspects of the Individual to analyse or predict certain aspects concerning his/her performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement

3.3 Data transfer:

Prior to agreeing to grant access (via transfer or remote access) to the Personal Data to any processor outside the Kingfisher Group:

- we must ensure that the processor to whom we transfer Personal Data complies with this Standard and the applicable laws;

- we must identify and always record the following information: (i) the name and contact details of the processor's representative and of the data protection officer, (ii) the categories of data processed, (iv) the categories of Individuals whose data will be processed, (v) the address of the location(s) the data will be transferred to / accessed from, (vi) the list and corporate information of any subprocessors and (vi) the categories of recipients to whom the Personal Data have been or will be disclosed;
- we must ensure no Personal Data is transferred to/accessed from another country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals in relation to the processing of personal data or that a written contract containing adequate assurances is signed between the parties (or alternative arrangements to provide such assurances, compliant with applicable data protection laws, are in place).

3.4 Data retention

Personal Data should not be kept longer than is necessary for the purpose for which it has been collected (section 3.1, above). This means that data must be destroyed or securely disposed of from company systems when it is no longer required.

Example: A customer has entered a competition to win a new power tool by completing a form with his name, address and telephone number and has ticked a box to state that he does not want to receive any further communication from the Group Company. Once the draw has taken place the Group Company should delete the customer's details submitted on the form as it is no longer required for the purpose for which it was obtained.

The Kingfisher policy on document retention and the laws regarding retention time must be complied with.

3.5 Rights of the Individuals

Data must be processed in line with Individuals' rights. Individuals' rights vary according to the country. In the European Union, Individuals broadly have a right to:

(a) withdraw consent to the processing of their Personal Data (if the processing is being carried out on the basis of consent);
(b) object to processing of their Personal Data (if the processing is being carried out on the basis of legitimate interests);
(c) get access to any Personal Data held about them;
(d) have any inaccurate Personal Data rectified;
(e) have their Personal Data erased from the company's systems;
(f) have their personal data transferred to other companies;
(g) prevent processing that is likely to cause damage or distress to themselves or anyone else.

3.6 Complaint and breaches

Any complaints and breaches including any breach in security affecting Personal Data, must be reported immediately to the Data Protection Officer (dpo@kingfisher.com) and/or any Data Protection Lead (https://www.kingfisher.com/content/dam/kingfisher/Corporate/Documents/code-of-conduct/Data_Protection_Team.pdf).

Any complaints for breach in security affecting Personal Data, must be reported immediately to the Head of IT Governance (via https://kingfisher.service-now.com/navpage.do).

Any theft, misuse or breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data to must be immediately (and, in any event, within no more than 2 hours) reported to the Data Protection Officer and the Head of IT Governance.

4. Monitoring and Audit

Periodically an audit of compliance with this Policy Standard and the other data protection-related processes and rules issued by the Data Protection Officer or the Data Protection Leads will be conducted to ensure compliance with this Policy Standard.

If you are in any doubt as to the subject matter of this Policy Standard you should seek advice from the Group Data Protection Officer or your Data Protection Leads.

You may also use the whistleblowing hotline to report your concerns.

5. Overview of Consents and Approvals

Action / situation	Communication		To/by whom?
	(Prior) Notification	Prior Approval	
Data Breach	X		Group Data Protection Officer* + Head of IT Governance
Automated decision-making (including Profiling)	X	X	Group Data Protection Officer + Head of IT Governance
Data subject complaints	X		Group Data Protection Officer or Data Protection Leads
Regulatory enquiries	X		Group Data Protection Officer + Group Legal Director
Regulatory enforcement action	X		Group Data Protection Officer + Group Legal Director
Exercise of data subjects' rights	X		Data Protection Leads
New processing activities triggering requirement for Data Privacy Impact Assessment	X	X	Group Data Protection Officer + Head of IT Governance

*In all cases, either directly or through country Data Protection Lead.