Policy Statement

Kier complies with all applicable laws in connection with processing data, including the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018. Our data protection standards are underpinned by this policy as well as our Code of Conduct. Data users are obliged to comply with this policy when processing personal data.

Data Protection Definitions

- Data is information which is held electronically, or in structured paper-based filing systems.
- Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data.
- Personal Data means data relating to a living individual who can be identified from that data (or in combination with other information in our possession). Personal data can be factual (such as a name, employee number or date of birth) or it can be an opinion about that person, their actions and behaviour.
- Data Controllers are the decision makers over the processing of personal data. They exercise control over the purposes and means of any processing.
- Data Processors process personal data on the instruction of a data controller.
- Data Users are those employees (hereafter referred to as those people employed by Kier and those working on Kier premises/infrastructure and where Kier policies are applicable) whose work involves processing personal data.
- Processing is any activity that involves use of the data. It includes collecting, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to other parties.

- Special Category Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic data or biometric data, physical or mental health or condition or sexual life or sexual orientation (and such other categories as may be added from time to time). Special category personal data can only be processed under certain conditions.
- DP Legislation refers to any current or future laws or directives that are or will be applicable in the UK with respect to data processing. This includes the Data Protection Act 2018 and the UK General Data Protection Regulation.

Data protection principles

Anyone processing Personal Data must comply with the seven principles for processing Personal Data as are contained within DP Legislation. These provide that Personal Data must be:

Processed fairly, lawfully and transparently;

Personal Data must be processed in a way that is not unduly detrimental, unexpected or misleading. Personal Data may only be processed if there is a legal ground for that processing. One of the following conditions must be met:

i. Performance of a contract (for example, an employment contract in respect of Kier employees or a service contract in the case of services to clients)
ii. Legal obligation (where Processing is required to comply with a common law or statutory obligation)
iii. Legitimate interest (applicable where Kier or the wider society or the Data Subject(s) have a benefit in processing Personal Data and where such processing is balanced against the rights and freedoms of individuals)
iv. Consent (where the Data Subjects have given their permission to process their Personal Data)

If the processing you are considering does not fall under one of the conditions above, then contact Group Compliance for further guidance.

Personal Data must be processed in an open and honest manner. Individuals must be informed as to how their data is processed.

When Special Category Personal Data is required to be processed, additional conditions to those set out above must also be met. If you are intending to process Special Category Personal Data, please contact Group Compliance.

Processed for a specified purpose(s)

- The purpose(s) of the Processing must be clear from the start and must be recorded.

Minimised;

- The data collected must be adequate, relevant and limited to what is necessary to fulfil the stated purpose(s) of the Processing.

Accurate;

- Steps must be taken to maintain the accuracy of data, including correcting information that is incorrect or misleading. Kier employees are responsible for checking and updating their Personal Data held on the self-service portal on Oracle and must notify askHR immediately of any changes to their personal circumstances.

Not kept longer than necessary for the purpose; and

Processed securely.

- All Personal Data is classified as 'Confidential' (information that must not be disclosed unless appropriate). This principle means that Personal Data must be kept secure by maintaining the confidentiality, integrity and access to the data. Data Users must employ reasonable security measures

including, where appropriate and/or relevant:

i. Access control (into a building and/or floor)
ii. Physical storage locking controls
iii. Electronic folder restrictions

iv. Encryption
v. Kier-approved file transfer methods
vi. Secure Personal Data destruction

In complying with this principle Data users are required to adhere to the Kier Information Security Policy.

Personal Data must be processed in a manner that will enable the Kier Group to demonstrate accountability in meeting each of the six principles.

Transferring Personal Data outside the UK

Group Compliance must approve where a transfer of Personal Data outside the UK is being proposed. Personal Data may only be transferred out under certain conditions, including ensuring that Data Subject rights are maintained.

Data sharing

Personal Data may be shared with any entity within the Kier Group, or externally, only on a 'need to know' basis and so long as the Data Subject is informed.

Personal Data may only be disclosed externally if there is a legal basis (for example, a legitimate interest, legal obligation or to comply with a contract) to do so. We may also disclose Personal Data we hold to third parties:

a. In the event that we buy or sell any business or assets, in which case we may disclose Personal Data we hold to the prospective buyer or seller of such business or assets.
b. If our, or substantially all of our assets, are acquired by a third party, in which case Personal Data we hold will be one of the transferred assets.

Before sharing Personal Data, there are a likely to be a number of factors that the Data User must consider before sharing it. Some or all of the following factors will likely need to be considered before sharing Personal Data:

a. The objective – this will help to provide clarity on what data needs to be shared, if any, and to whom.
b. Data required – the data that is shared must be minimised to the data that is required
c. Recipients of data – data should only be shared on a 'need to know' basis
d. Frequency of data sharing – Personal Data should not be shared more frequently than necessary. Data users must consider whether it is appropriate to share data on an exceptional basis, on-going or routinely
e. Mode of sharing – data must be shared in a secure manner
f. Risk of sharing Personal Data – data users should consider risks to the Data Subjects
g. Anonymising data – data users should consider if the objective can still be achieved by anonymising data
h. Transfer of data outside the UK – Personal Data must not be transferred outside the UK without authorisation from Group Compliance

Data transmission

Data transmission is the transfer of data from one location to another. It comprises the transmission of physical data and electronic data.

Physical transfer of data carries with it greater Personal Data risk due to the inherent lack control in the event of a potential data breach. Accordingly, physical data transfers should only be carried out where there is no electronic alternative available or if it would not be practical to transfer the data in another manner.

The duration of the transit period, when transferring from one Kier location to another, should be kept to a minimum to lower the risk of a potential data breach.

Physical data that is required to be posted must be sent in a secure manner. This will typically be via point- to-point Courier or in accordance with agreed business unit protocols.

Where electronic transfer is appropriate, it is required to be transferred securely and through a Kier approved means of transfer such as OneDrive (or, in some cases, by use of an FTP server).

Data Retention

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. Reference should be made to the Kier Document Retention policy. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required.

Video images - CCTV

CCTV is generally regarded as a privacy intrusive method of monitoring and should therefore only be considered for use once other alternative options (that may be less intrusive) have been considered and are deemed unsuitable. The appropriateness of any CCTV systems that are already in operation, should be reviewed periodically to check that its use remains appropriate and that it meets the purpose for which it was installed.

Two examples (not directly relevant to our services) are provided to provide guidance on the approach expected by the regulator:

Example 1: Cars in a car park are frequently vandalised and broken into at night. Consider whether improved lighting might be an effective solution and remove the need for CCTV.

Example 2: CCTV is justifiably in place at a site adjacent to a park as a security response to anti-social behaviour. Some months later, the park is closed and is replaced by a block of flats. Review whether CCTV is still needed for the original purpose.

Before installing CCTV, your Service Owner must be contacted and data privacy risks must be assessed.

The system must be operated in a way that is consistent with the rights and freedoms of individuals (i.e. does not cause harm to individuals).

CCTV must be located at strategic points and must be focussed/positioned to capture images of interest.

In the case of static CCTV, these should be pointed towards or in the immediate vicinity of Kier property (or the property of the client where we are working) or, where operated on vehicles, specifically towards the area that is the focus of the monitoring.

Appropriate legible signs must be placed in prominent locations to inform those whose images may be captured that CCTV is in operation.

Designated owners (or a delegate) of the CCTV system must complete the checklist for installation and maintenance of CCTV systems.

Drones

Drones may be operated in limited circumstances and in certain locations. The primary purpose of operating drones must be in connection with enhancing commercial operations rather than a collection of Personal Data.

Users are required to comply with all applicable laws (including those from the Civil Aviation Authority) relating to the use of unmanned aircraft and any licencing requirements. Where specific permissions are required, users are required to obtain and comply with those permissions.

Before considering use of drones contact your Service Owner. Data privacy risks must also be assessed.

Data Subject's rights under DP Legislation

We will process all Personal Data in accordance with Data Subjects' rights where it is applicable, and in particular their right to:

a. request to have inaccurate data amended
b. request access to any data held about them by a data controller
c. be informed about how their Personal Data is processed
d. prevent the processing of their data for direct-marketing purposes

e. object to the processing of their Personal Data in certain instances
f. restrict the processing of their Personal Data in certain instances
g. withdraw their consent in the case where consent had previously been granted
h. request erasure in certain instances

With exception to (a) Data Users must consult with Group Compliance (compliance@kier.co.uk) to consider the request from the Data Subject(s). In most cases, we are required to comply with any Data Subject request within one month of the request being submitted. In the case of (a) data users should proceed with the request to have information amended without consulting with Group Compliance.

Information Commissioner's Office (ICO) registration

The ICO maintains a public register of all data controllers registered to process Personal Data. The Group Company Secretarial team is responsible for ensuring compliance with the requirement to manage and maintain the notifications made to the ICO in respect of data controller registration. However, it is the responsibility of the financial director (or their equivalent) of each Kier entity to inform the Company Secretarial team whether registration is required or of any changes to that data controller's turnover so that the correct ICO registration fee is paid (or de-registered as the case may be for businesses that are no longer operational).

Data breaches and complaints

A potential data breach is an incident in which sensitive, confidential or otherwise Personal Data has been accessed, disclosed or handled in a manner inconsistent with the intended treatment of that information.

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes.

A non-comprehensive list of potential data breach examples includes:

- Unauthorised deletion of data
- Sending data to an unintended recipient
- Access to data by an unauthorised individual
- Sending Kier confidential data to a personal email address for non-business use
- Loss or theft of a laptop
- Alteration of data without permission
- Misplacing data
- Cyber attack

Data breaches may also include cases where Data Subjects' rights (noted in section 10) are not managed appropriately.

It is important that we are able to deal with any data incident as soon as possible to effectively manage the incident. As such, all Kier Group employees must notify the Group Data Protection Officer (DPO) at compliance@kier.co.uk, immediately after becoming aware of any data incident. In no circumstances should you communicate details of the incident outside of those managing the data security incident without first contacting the DPO.

The DPO, and a team compiled by the DPO (including, where appropriate, the Kier Group Head of Information Security, and a representative from the relevant business unit/function) will consider the potential data breach facts as presented. The DPO will determine the course of action to take according to the findings.

This Policy should be read in conjunction with the Chief Executive Foreword which includes the whistleblowing contact information.

For and on behalf of Kier Group plc

Andrew Davies, Chief Executive

November 2024