Knight Frank Global Data Protection Policy

Purpose

This policy sets out Knight Frank's approach to the management of data protection and privacy. It applies to all processing of personal data across Knight Frank.

What is personal data?

For the purposes of this policy, personal data means any information relating to an identified or identifiable individual. An individual may be identifiable directly or indirectly through identifiers such as a name, identification number, location data, an online identifier, or factors relating to their physical, physiological, genetic, mental, economic, cultural or social identity.

Processing personal data refers to any operation carried out on that information, whether automated or manual. This includes activities such as collecting, recording, organising, storing, adapting, retrieving, consulting, using, disclosing, aligning or combining, restricting, erasing or destroying personal data.

Why it Matters

The Group Executive Board, (The Board) and Management of Knight Frank LLP are committed to protecting the personal data and respecting the privacy of individuals.

We will apply the data protection principles contained in the UK GDPR as our standard approach globally. Where local law or regulation conflicts with these principles then local law will override the specific aspect of the UK GDPR which is in conflict.

Knight Frank is a data controller for processing activities where it determines the purposes and means of the data processing. This includes most processing of employee data and client data when acting on Knight Frank commercial interests. When acting as a data controller, we will comply with the data protection principles contained in the UK GDPR.

Scope

This policy applies to all employees of Knight Frank. It applies also to consultants, contractors and agency workers in relation to their work for, or on behalf of, Knight Frank.

Knight Frank refers to the member firms of the Knight Frank global network, each of which is a separate legal entity. The Knight Frank global network comprises Knight Frank LLP, its subsidiaries (direct or otherwise), its affiliates and any other entity or practice carrying on business under or including the name Knight Frank or in association with Knight Frank LLP internationally in over 50 territories.

Failure to comply with this policy may result in disciplinary action being taken against anyone involved, or the termination of contracts with contractors and other third parties working for Knight Frank.

The Knight Frank global network can use the Knight Frank name and resources of the network. Member firms agree to abide by certain common policies and to maintain the standards of Knight Frank.

General Principles

Knight Frank will process personal data in compliance with the following six data protection principles.

1. Lawfulness, fairness and transparency

We will only process personal data where it is lawful.

We will identify all data processing activities across the business and record these in a Record of Processing Activities (RoPA). Each processing activity will be assessed against the lawful bases set out in section 5.

Our Privacy Notices set out information about our data processing, such as the types of information we collect, our purposes for processing, who we share personal data with and the retention periods.

2. Purpose limitation

We will only collect personal data where we have a specified, explicit and legitimate purpose.

We will not process personal data for any purpose which is incompatible with the original purpose. When processing personal data for a new purpose, we will conduct a compatibility assessment.

3. Data minimisation

We will only process personal data that is adequate, relevant and limited to what is necessary to achieve our purpose.

4. Accuracy

We will take reasonable steps to ensure that the information we hold is accurate and up to date.

5. Storage limitation

We will not keep personal data for longer than is necessary to achieve our purposes.

Our Retention Policy and Schedule set out the assigned retention periods relating to types of data and how we will delete or dispose of the personal data that we hold.

6. Integrity and confidentiality

We will implement appropriate technical and organisational security measures to ensure the security of the personal data we process.

The technical measures we employ will be set out in our Information Security Policy.

The organisational measures we employ include:

- Allocating responsibility for data protection compliance to relevant individuals
- Providing appropriate and relevant data protection training to anyone who handles personal data on an annual basis.
- Developing policies and procedures on relevant areas of compliance to give everyone clear direction about what steps to take in certain situations, for example data breaches and Data Subjects Rights requests.

Our Data

All data used, collected, developed or created by Knight Frank, its consultants, contractors and agency workers in relation to their work for, or on behalf of, Knight Frank, including, but not limited to, documents, templates, databases and client or counterparty information (“Data”), is the property of Knight Frank LLP.

Data must not be transferred outside of Knight Frank's IT Environment except:

- where it is necessary to meet our contractual commitments to clients,
- for the purposes of marketing our services
- to facilitate the delivery of services to Knight Frank by approved third party suppliers and partners who have entered into a contract with Knight Frank, or
- where mandated by regulators or other legal authorities.

Under no circumstances should Data be transferred for any purpose other than as set out above. Prohibited use of Data includes, but is not limited to, transferring Data to an employee's (or their friends’ or families’) personal storage or email service, third party computer, or those of a competitor of Knight Frank.

The exception to this prohibition is where employees are handling their own personal data that has been generated in the course of their employment—such as pay slips, pension information, health insurance documents, or other employment-related records**.** Employees may download or store such personal data outside of the Knight Frank environment solely through authorised channels and using the approved method provided by the business. Employees must not extract, forward, or store this information by circumventing approved systems, and must ensure that any external storage complies with the security guidance issued by Knight Frank.

Breach of this policy may result in disciplinary action up to and including dismissal.

Accountability

We will allocate responsibility for data protection compliance to the Data Protection Officer or designated senior individual responsible for data protection..

We will demonstrate compliance with the data protection principles by maintaining appropriate documentation and making these available where necessary, for example a RoPA and Data Protection Impact Assessments.

We will monitor compliance with data protection across our business by conducting audits and producing reports highlighting areas of non-compliance.

We will report data protection compliance to senior management and relevant committees including the Risk Steering Committee Information Security and Privacy Group, and the Board.

We will develop a suite of data protection KPIs to monitor compliance with data protection obligations including data breaches, rights requests and training completion rates.

Roles and Responsibilities

All employees – All employees are responsible for complying with this policy and all other guidance and training relating to data protection provided by Knight Frank. All employees must report any data protection issues they come across (including data breaches) to either their line manager or the Data Protection Team.

Data Protection Officer (DPO) – The DPO and the Data Protection Team are responsible for monitoring compliance with data protection legislation, reporting areas of non- compliance and making recommendations to improve compliance. The DPO will conduct activities to improve the data protection compliance across Knight Frank including providing expert advice, training where necessary and maintaining documentation of processing activities and risk assessments.

Risk Steering Committee– The relevant regional Risk Steering Committee is responsible for reviewing data protection risks reported by the Data Protection Team and monitoring mitigating actions. The Risk Steering Group will be responsible for operationalising any actions arising from these risk reviews, ensuring that appropriate measures are implemented across the business.

Information Security and Privacy Group (ISPG) – The ISPG is responsible for implementing technical measures to ensure the security of personal data.

Board – The Group Executive Board (The Board) is ultimately responsible for compliance with data protection legislation across Knight Frank. The Board will ensure that appropriate resources are allocated to support data protection compliance.

Lawful basis

In line with the lawfulness, fairness and transparency principle, we will ensure that all data processing activities are allocated an appropriate lawful basis. The lawful bases are as follows:

- Where we have obtained the data subject's consent, we will ensure that it is a freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by clear affirmative action, signify agreement to the processing of their personal data. We will keep records to demonstrate that we have obtained valid consent, including when it was given and by what means. We will ensure that data subjects have a right to withdraw consent at any time.
- Where the processing is necessary for the performance of a contract with the data subject, or to enter into pre-contractual negotiations.
- Where the processing is necessary to comply with a legal obligation.
- When relying on a legal obligation, we will ensure that we can point to a clear and defined statutory, regulatory or common law obligation which compels us to process personal data in that way.
- Where the processing is necessary to protect the vital interests of an individual, e.g. to protect someone's life.
- Where Knight Frank has a legitimate interest in processing the personal data that outweighs the privacy interests of the data subject. When relying on legitimate interests, we will conduct a Legitimate Interest Assessment (LIA) to evidence that we have appropriately assessed the balance between the interests of

the business and the interests of the data subject.

Special category and criminal offence data

Special category data are types of personal data that require higher levels of protection as there is a higher risk of harm to the data subject. Special category data consists of the following types of personal data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning a person's sex life
- Data concerning a person's sexual orientation

We will ensure that we have an appropriate lawful basis under Article 9 of the UK GDPR to process special category data.

Criminal Records Data

Criminal records data refers to information relating to criminal allegations, investigations, proceedings, or convictions. Although this type of information may be governed by different legal requirements across jurisdictions, it is widely recognised as highly sensitive and requiring enhanced safeguards due to the potential impact on individuals' rights, freedoms, and wellbeing if mishandled.

We will only collect and process criminal records data where it is **lawful, necessary, and proportionate** to do so, and only for legitimate business purposes such as employment screening where permitted, compliance with regulatory or legal obligations, safeguarding, security, or the prevention and detection of unlawful acts.

To protect this type of data, we will ensure that:

- Processing is limited to authorised purposes and occurs only when required under applicable laws or legitimate organisational needs.

- Access is restricted to employees with a clear and justifiable role based purpose, subject to confidentiality obligations.

- Appropriate organisational, technical, and security measures are applied to prevent unauthorised access, disclosure, alteration, or misuse.

- Criminal records data is retained only for the minimum period necessary for the purpose for which it was collected, after which it will be securely deleted or anonymised.

- Additional documentation, safeguards, or impact assessments will be implemented where required by local law or internal policy.

Use of Artificial Intelligence (AI) Technologies

Knight Frank may implement Artificial Intelligence (AI) technologies to support internal operations, enhance workplace productivity, and improve the delivery of our services. These technologies may be used for a variety of functions, including but not limited to document generation, communications support, meeting transcription, and data analysis.

AI tools may, in some cases, process personal data relating to employees, clients, or other individuals. Any such processing must be carried out in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act, and must be based on a valid legal basis, such as:

- **Legitimate interests**, where AI enhances operational efficiency or service quality without infringing on individuals' rights and freedoms;
- **Consent**, where required for specific AI applications;
- **Performance of a contract** or **compliance with a legal obligation**, where relevant.

Where AI technologies are used to process personal data, they must be subject to appropriate **Data Protection Impact Assessments (DPIAs)** and implement effective technical and organisational safeguards, including but not limited to data minimisation, access controls, encryption, and secure retention practices.

AI systems must not be used to make solely automated decisions that produce legal or similarly significant effects on individuals without meaningful human intervention, except where explicitly permitted by law and with appropriate safeguards in place.

- All employees are expected to use AI tools responsibly and in accordance with this policy and:The Artificial Intelligence Policy
- The Information Security Policy

Data protection rights

We will comply with data protection rights exercised by individuals.

We will manage data subject rights requests in line with our Rights Requests Procedure.

We will respond to all rights requests within one calendar month unless data protection law allows for this to be extended.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making.

Data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Data Breach Procedure sets out the steps we will take to manage data breaches when they occur.

We will keep a record of all data breaches, incidents and near misses we become aware of to identify any trends. We will implement mitigating actions to prevent potential data breaches from occurring.

Data processors

Knight Frank employs data processors to process personal data on our behalf. This includes where business functions are supported by suppliers or third-party systems and personal data is shared with them.

Where we employ data processors, we will take the following actions to ensure that the data processor is processing personal data securely and lawfully:

- We will enter into a contract with the data processor which contains appropriate terms to ensure that data is processed lawfully and securely.
- We will conduct due diligence on potential data processors in line with the procurement process to ensure they implement appropriate technical and organisational security measures to keep personal data secure.

- We will conduct regular checks on our data processors to ensure their technical and organisational measures remain sufficient.

Knight Frank as a data processor

Knight Frank is a data processor where it is employed to process personal data on behalf of another entity. This includes where Knight Frank provides IT services to other companies, such as licensees. When acting as a data processor, we will ensure that a contract is in place with the data controller setting out the relevant data protection terms, including our documented instructions for processing the personal data.

International transfers

We will ensure that any transfer of personal data outside the UK is conducted lawfully by ensuring that either:

- An adequacy decision has been granted for the country where personal data is being transferred.
- Standard Contractual Clauses are in place with the recipient of personal data and a Transfer Impact Assessment (TIA) has been conducted.
- An International Data Transfer Agreement (IDTA) is in place with the recipient of personal data and a Transfer Risk Assessment (TRA) has been conducted.
- Binding Corporate Rules (BCRs) are in place.
- Knight Frank has implemented a Group Data Transfer Agreement (GDTA) which allows us to transfer data across jurisdictions with our other entities and partners across the globe for a limited set of circumstances.

Privacy by Design

We will implement a culture of privacy by design.

We will achieve this by carrying out tailored and specific training to teams that design systems and processes to ensure that privacy is at the centre of decision making.

We will be conducting Data Protection Impact Assessments on high-risk data processing and on systems, projects and processes that pose a data protection risk.

Direct marketing

Direct marketing is communication directed to particular individuals with the purpose of marketing commercial products and services or the promotion of aims and ideals of the business.

We will only conduct direct marketing via electronic means where we have the consent of the individual, unless the soft opt-in exemption applies.

We will only conduct direct marketing via post where we have the consent of the individual, or we have a legitimate interest in conducting the marketing.

Whistleblowing

Knight Frank maintains a Global Whistleblowing Policy, incorporating an independent hotline, to ensure that anyone can report concerns, confidentially where possible, and to ensure that such concerns are investigated and remediated appropriately.

Anyone who has concerns relating to a potential breach of this policy must follow our whistleblowing policy and report the matter immediately. There will be no repercussions for employees or associated persons taking these reporting steps, providing the suspicions or concerns are for genuine and not malicious reasons.

Management has a responsibility to investigate any reports of wrong-doing. Inaction in investigating reported or known issues will not be tolerated and will be subject to disciplinary action.

Policy implementation

This policy is to be adhered to by all entities part of the Knight Frank Global Network. This policy will be made

available to the Knight Frank Global Network via the Knight Frank website and other applicable platforms.

Monitoring and Review

This policy will be reviewed in line with all other global policies at least annually. If there is a business or legislative reason for it to be reviewed more frequently, then this will be conducted by the UK Best Practice team.

Knight Frank Group Data Protection Policy

Prepared: April 2026
Exec Sponsor: William Beardmore-Gray
Position: Senior Partner and Chairman
Review Date: April 2027