Section F.3
Issue date: 01/04/18
Updated: 12/03/21
Responsibility: Head of Data Protection Compliance

Policy
Skanska UK
Data Protection

This Policy applies to all Employees (as defined below) of Skanska, as well as Supply Chain Partners (as defined below).

It is the responsibility of all Employees (and Supply Chain Partners) to assist Skanska to comply with this policy and to familiarise themselves with this policy and apply its provisions in relation to all processing of personal data.

The policy covers all personal data in any form, including but not limited to electronic data, paper documents and disks and all types of processing, whether manual or automated that is under Skanska's possession or control.

Skanska complies with the data privacy laws of the countries in which it operates, regulations and guidance documents in those respective countries, as well as applicable data transfer obligations. Skanska will also apply this policy to the maximum extent possible across Skanska, except where local requirements contradict with, or are more onerous than those set out in this policy, in which case those local requirements will be followed.

As set out in Skanska's Code of Conduct it is the policy of Skanska to take all necessary steps to ensure that personal data (as defined below) Skanska holds about its employees, customers, suppliers and all other individuals is respected, kept safe and secured, processed (as defined below) in a fair and lawful manner and in compliance with all applicable data privacy laws.

It is the policy of Skanska to ensure that all relevant statutory requirements are complied with and that Skanska internal procedures are monitored periodically to ensure compliance.

Skanska has separate documents covering the processing of special category data and criminal record data and these documents should be read in conjunction with this policy document.

1 Purpose

Skanska has adopted this Data Protection Policy ("Policy") to provide general overarching guidelines to ensure that Skanska is aware of its data protection compliance obligations.

This policy is not intended as a definitive statement of the application of all applicable data privacy laws; instead it acts as a general framework of best practice, setting out the principles of data privacy adopted within Skanska to assist in the application of this Policy.

This policy is based on the Data Protection Act 2018 and the UK General Data Protection Regulation ("UK GDPR").

2 Definitions

Criminal Record Data shall mean any information relating to criminal convictions and offences.

Data Processor shall mean a legal entity who processes personal data on behalf of the Controller.

Data Controller shall mean the legal entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Protection Act 2018 shall mean the framework for the data protection law in the UK which sits alongside and supplements the UK GDPR

Data Subject shall mean an identified or identifiable natural person whose personal data is being processed.

Employees shall include all contractors, consultants, temporary and permanent employees of Skanska.

Informed Consent shall mean that the individual agrees to the processing of his or her personal data by a clear affirmative act that is freely given, specific, informed and unambiguous.

Personal Data shall mean any information relating to an identified or identifiable natural living person; an identifiable natural person is one who can be identified directly, or indirectly via use of other information. Examples include name, address, birth date, employee number, photographs, IP address, health data, geographical location and movements, online activities, behaviour patterns.

Personal Data Breach shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing shall mean any operation or set of operations performed on personal data or on sets of personal data, whether or not performed by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, erasure or destruction.

Special categories of personal data shall mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or a person's sex life or sexual orientation.

Supply Chain Partners shall mean a third party (i.e. supplier / service provider) who receives from Skanska or who is otherwise entrusted with personal data on behalf of Skanska.

UK GDPR shall mean the UK General Data Protection Regulation which are based on the EU GDPR and which sit alongside the Data Protection Act (2018). The regulations set out the key principles, rights and obligations for most processing of personal data.

3 Data Protection Principles

Skanska will comply with the following principles which promote good conduct in relation to the processing of personal data:

- Personal data will be processed in a fair, lawful and transparent manner;
- Personal data will be obtained for specified, explicit and legitimate purposes and will not be further processed in any manner incompatible with those purposes;
- Personal data will be adequate, relevant and not excessive in relation to the purposes for which it is processed;
- Personal data will be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that Personal Data that are inaccurate (having regard to the purpose (or purposes) for which they are processed) are immediately deleted or rectified; and
- Personal data processed for any purpose (or purposes) will not be kept in a form which permits identification of Data Subjects for longer than is necessary for the purpose (or purposes) for which the Personal Data is processed.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal Data will at all times be processed in a manner that can demonstrate compliance with the above-mentioned principles.

4 Data Protection Requirements

When considering how the data protection principles and overarching requirements apply to the personal data processed, it is important to keep in mind that Skanska may act as Data Controller in certain situations and Data Processor in others. For example, Skanska acts as data controller when it processes the personal data it collects from its employees, and it acts as data processor when it processes the personal data of its customers' customers. Skanska may also act as a joint data controller with another data controller.

Where Skanska acts as Data Processor for its customers, it acts on the instructions of its customers, which means that Skanska is reliant on its customers to tell it how we should use/process their personal data. For example, if a customer receives a data subject access request from one of its Data Subjects, Skanska's customer may ask the business to assist it complying with the request and/or Skanska may be under a contractual obligation to assist them.

The following overarching requirements set out how personal data should be treated.

4.1 Notice to Data Subjects (also known as a privacy or 'fair processing' notice)

Data Subjects must be informed about how their personal data is used, including about the types of data collected, the purposes for which the data is collected, anyone to

whom their personal data may be disclosed outside of Skanska, the identity and contact details of the Data Controller, where applicable, the fact that the Data Controller intends to transfer personal data outside the EEA with reference to the safeguards in place, and the rights available to the Data Subjects.

Relevant Data Subjects for the purposes of Skanska will include employees and other third parties. Skanska satisfies this requirement in two ways:

.

- Via an Employee Privacy Notice, which is issued to all Employees via the UK Data Protection page on OneSkanska and to all new employees with their offer pack;

- In Skanska's Terms of Use and Privacy Policies, which are external-facing notices, made generally available on Skanska websites under Terms of Use.

In certain circumstances, short-form privacy notices may be presented to Data Subjects and included on data collection forms, internet portals etc. These should include a link to the main Privacy Policy, as appropriate.

4.2 Fair and lawful processing

The way in which personal data is held and used must be kept consistent with the privacy notice provided to the Data Subject.

No further or alternative use should be made of the personal data without first considering the need to identify a legitimate reason for the change, and/or issuing an updated privacy notice.

If Skanska is considering implementing a new project or way of working or making changes to an existing project or way of working, which will involve the processing of personal data, it is important to consider (and record) the condition which can be relied upon together with the rationale for the processing.

All processing of personal data must be justified by reference to one of a number of lawful bases for processing. These are:

- The processing is required for compliance with a legal obligation to which Skanska is subject;
- The processing is required for the performance of a contract to which the data subject is party;
- The processing can be performed on the basis of the legitimate interests pursued by the controller;
- The processing can be performed if the data subject has given his or her consent to it;
- The processing is necessary to protect the vital interests of the Data Subject; and
- The processing is necessary to perform a task carried out in the public interest or in the exercise of official authority.

The processing of Special categories of personal data requires additional justification and may not be processed without prior consultation with the HR Risk and Compliance Team.

Skanska's GDPR team maintains a *Data Register* which records certain details about all business processes which use personal data and special categories of data, including the lawful basis for each such business process. If any part of Skanska considers implementing a new project or way of working or making changes to an existing project or way of working, which will involve the processing of personal data, it is important to consider (and record) the lawful basis which can be relied upon together with the rationale for the processing. The Data Register may need to be updated to reflect the new or revised project or way of working. Employees are required to contact their GDPR OU representative to notify them of any updates need to be made.

In addition, in such situations, consideration should be given to whether a data protection impact assessment should be carried out. Refer to the Data Protection Impact Screening Questions template on the UK Data Protection page to determine if a full Data protection Impact Assessment is required.

Where Skanska processes personal data on behalf of customers, it is each of Skanska's customer's responsibility to ensure that the processing Skanska undertakes on its behalf is justified by reference to a lawful basis for processing. Further, it is the responsibility of Skanska's customers to ensure that their Data Subjects are informed about how their personal data will be used and that actual usage is in line with their privacy notice.

Where Skanska engages a third party to process personal data on its behalf, UK GDPR compliant contract clauses must be used to ensure the security and integrity of the data.

4.3 Proportionality

The nature and type of personal data held must be proportionate and necessary for the purpose for which it is to be required.

There should be a clear business justification, or legal need to hold the specific types of personal data that are collected from individual Data Subjects. Care must be taken to avoid collecting excessive or irrelevant elements of personal data or allowing personal data to be used for purposes that cannot be justified as 'necessary'. Advice should be sought from the HR Risk and Compliance Team as it may be unlawful to collect the personal data from the Data Subject if the data principles are not followed.

5 Data sharing / transfers

5.1 Sharing personal data outside of Skanska

Personal data should only be disclosed outside Skanska where there is a legitimate business need or overarching legal justification to do so. Disclosure must be made on a strictly limited 'need to know' basis where there is clear justification for transferring personal data: either because the Data Subject has consented to the transfer or because it is for a legitimate business need.

In each case, Data Subjects must be aware that the transfer or disclosure is likely to take place to a 3rd party (such as a Supply Chain Partners). This should normally be achieved using Skanska's external privacy notices, except where the transfer or disclosure is clearly understood by the Data Subject as a necessary part of a function of Skanska. Assurances should also be sought from the 3rd party recipient that they will only use the personal data for legitimate / authorised purposes and keep it secure.

If a particular disclosure is required to meet a legal obligation (for example to a government agency or police force/security service) or in connection with legal proceedings, the personal data may be provided so long as the disclosure is limited to that which is legally required.

The HR Risk and Compliance team must be consulted if personal data needs to be shared, as they will provide advice on the appropriate way to share personal data.

5.2 Transferring personal data overseas

Generally, personal data originating in the UK must not be transferred outside of the UK or EEA, unless there is a mechanism for ensuring adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

Be aware that transfers may take place that are not obvious. For example, if a Supply Chain Partner located in the UK sub-contracts some of its processing obligations to a 3rd party outsourced provider in India, there will be a transfer of personal data out of the UK and EEA, i.e. from the Supply Chain Partner (who is a data processor of Skanska) to the 3rd party outsourced provider (who is a sub-processor) which will be prohibited unless certain conditions are met.

Managing overseas data transfers in accordance with these principles requires particular care. Where any personal data is proposed to be transferred to another country or outside of the EEA, the HR Risk and Compliance team must be consulted who will advise on how to comply applicable data transfer restrictions.

6 Accuracy and retention

Personal data must be kept accurate, complete and up-to date and not retained for longer than the purposes for which it was collected unless there is a clear overriding business need or legal / regulatory requirement to retain the personal data. Skanska's Document Retention Policy and Document Retention Schedule (Section D.4.i) sets out the details for ensuring that documents/records are updated, archived and deleted appropriately.

Special categories of personal data, such as criminal convictions and ethnicity, must also be kept up to date and retained only for as long as possible. The *Document Retention Schedule* should be sought for further guidance.

Skanska retain personal data during the process of providing services to customers. It is important to note Skanska may be under customer-specific requirements in respect of the management/retention/disposal of such data due to these business relationships.

7 Rights of Data Subjects

Data Subjects have the right to:

- access their personal data;
- require rectification of any errors in their personal data;
- require deletion of their personal data if continued processing is not required;
- restrict the way in which their personal data is processed (including the purpose of

the processing);
- transfer their personal data between Data Controllers; and
- object to processing.

There are some exceptions to these rights. Refer to the Information Commissioner's Office (ICO) website or contact the GDPR inbox for more information.

Data Subjects must be provided with a reasonable opportunity to access their personal data at reasonable intervals for purposes of examining it, confirming its accuracy and amending it if it is incomplete or inaccurate. Data Subjects should also be provided with contact information to enable them to access a full copy of their personal data in accordance with their legal 'subject access rights'.

All requests from Data Subjects relating to how Skanska processes their personal data (for example requests to access to their personal data or cease processing their personal data) require careful consideration. Requests of this kind should be made via the GDPR inbox. Whereby an employee receives such a request in writing from another employee they must immediately refer it to the GDPR inbox without delay as the timescales for responding to such a request are short.

As mentioned above, where Skanska acts as a data processor and Skanska is asked by its customers to assist them to comply with data subject rights requests they receive from their Data Subjects, it is important that Skanska acts on the instructions of its customers and in accordance with any contractual requirements.

8 Security of personal data

Appropriate technical and organisational security measures must be taken to prevent unauthorised or unlawful disclosure or access to, or accidental or unlawful loss, destruction, alteration or damage to personal data.

Employees and Supply Chain Partners have a responsibility to help keep personal data secure. In particular, Employees should be aware of their obligations, and at all times follow Company recommendations, for example in the IT Acceptable Use policy (Section I).

All employees who have access to personal data are legally obliged to keep information confidential. Access and use of personal data must be limited on a strict 'need to know' basis.

Where personal data is transmitted outside Skanska, for example to Supply Chain Partners, a secure medium must be used to transmit such data and written agreements (containing the required level of security standards) should be in place with each such Supply Chain Partners. As set out above, if personal data is needed to be transferred outside Skanska, the HR Risk and Compliance team must be consulted who will provide advice on the appropriate way to share personal data.

9 Personal data breaches

All personal data breaches should be contained and remedied as soon as possible. In the event of a personal data breach, the Data Controller must notify the appropriate supervisory authority, usually the ICO, without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach (unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons). A Data Processor must notify the Data Controller of any personal data breach without undue delay after becoming aware of it.

Examples of personal data breaches include 3rd party attacks on IT infrastructure designed to harvest personal data for criminal purposes, accidental loss or theft of Skanska devices (e.g. mobile phones, laptops, USB devices) where the personal data is not suitably encrypted and the passing to 3rd parties or disposal of personal information without appropriate security measures being in place.

All employees (and supply chain partners) have an obligation to report personal data breaches (or suspected personal data breaches) to the HR Risk and Compliance team who will make the decision on whether to notify the ICO. The Reporting Personal Data Breaches – Employee Guide provides further details on how personal data breaches should be managed and resolved. Employees should familiarise themselves with, and at all times follow, the plan in the event of a personal data breach.

If a personal data breach occurs and impacts on personal data Skanska processes on behalf of its customers, Skanska will need to notify the customer without undue delay. Furthermore, Skanska may be required to provide the customer with specific details relating to the personal data breach within a short timescale upon becoming aware of it. Refer to the Reporting Personal Data Breaches – Employee Guide document for more information.

10 Employee monitoring

Refer to the IT Acceptable Use Policy (Section I).

11 Direct marketing

Direct marketing is the transmission by any means (including post, telephone, email, SMS, direct messaging, fax etc.) of materials advertising or promoting Skanska's products and services to a specific individual (including where that individual is acting in a business capacity, for example the work email address of an employee of one of its customers).

The level of consent required to market to an individual will depend on the type of direct marketing activity to be undertaken and country specific privacy rules, which (in relation to electronic marketing) sit outside of the UK GDPR.

As a general rule, Data Subjects should only be contacted for marketing purposes by electronic means (i.e. email or text) if they have either expressly 'opted-in' to receiving communications in this way, or there is an existing commercial relationship and they are given the opportunity to 'opt-out' of marketing communications when Skanska first collects their details, and in all subsequent communications.

In all cases, Data Subjects must be given the chance to decline to receive direct marketing material and a suppression list should be held listing Data Subjects who have indicated that they do not want to be contacted in the future. Where telephone marketing is carried out, telephone numbers should be screened against the public suppression list maintained by the Telephone Preference Service.

12 Cookies

Skanska websites use cookie technology and maintains a statement explaining to users' which cookies are deployed by Skanska and their purpose. The statement gives users the opportunity to opt into certain categories of cookie if they wish. Any new use of cookies or other tracking technologies will necessitate an amendment to the cookie statement under Terms of Use.

13 Automated decision-making

Decisions should not be made about individuals using entirely automated processes. Advice should be sought from the HR Risk and Compliance Team before considering any techniques that will result in decisions being made about individuals through automated means, to ensure appropriate manual reviews are embedded into the decision-making process. This extends to automated processes which may be used for screening recruitment candidates, as well as profiling techniques used to automatically make decisions about policy applicants or claimants in underwriting and claims management contexts.

14 CCTV

CCTV systems should be operated with care to avoid disproportionate risk of privacy intrusion to individual Data Subjects. CCTV systems should be installed and operated in a way that is proportionate to the risks being covered and prominent notices should be displayed in the area covered by the CCTV system to make sure people are aware that the system is in operation. If considering installing a new CCTV system, or making any changes to an existing CCTV system, consult with the HR Risk and Compliance team.

15 Recordings

All employees have an obligation to follow data protection legislation when considering making recordings, whether video, audio, or both. If the recording is not for purely personal use, the person making the recording becomes a Data Controller and must comply with the requirements of a Data Controller detailed under current data protection legislation.

Prior to data processing (recording) the individual undertaking recording must assess the legal basis for processing the personal data, how the recording will be managed to keep it adequately secure and otherwise comply with the data principles. If consent is the lawful basis for processing the personal data this should be obtained prior to processing the personal data. The individual must also ensure they are storing and retaining the personal data correctly.

Employees are prohibited from making covert recordings.

16 Consequences of non-compliance

If Skanska is found to be in breach of applicable data protection laws, Skanska could face fines and enforcement action taken against it from data protection supervisory authorities. Employees and supply chain partners are also responsible for data protection. Failure to comply with this policy may lead to disciplinary action, up to and including summary dismissal for serious or repeated non-compliance.

17 Accountability for Skanska's actions

Periodic monitoring of adherence to this policy takes place to help ensure compliance with this policy, applicable data protection laws and/or contractual agreements in connection with the handling of personal data. Initially this will be undertaken once a year but Skanska retains the right to amend this schedule pending guidance from the ICO.

As set out earlier in this policy, it is the responsibility of all Skanska employees (and supply chain partners) to assist Skanska to comply with this policy. It is therefore key that all employees (and supply chain partners) familiarise themselves with both this policy and apply their provisions in relation to all processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal or, in the case of supply chain partners, termination of contract.

18 Complaints

Skanska is committed to resolving the legitimate privacy issues of its employees, supply chain partners, customers, suppliers and all other individuals. If any employee or supply chain partner discovers a breach of this policy, either through their own actions or actions of others, they must contact the HR Risk and Compliance Team via the GDPR inbox to report it. Alternatively, the Code of Conduct hotline can be used to report actions of others anonymously.

If an individual covered by this policy makes a complaint about the processing of his/her or someone else's personal data, and the complaint is not satisfactorily resolved through this internal procedure, then Skanska will co-operate with the ICO and comply with the advice of the ICO to resolve any outstanding complaints. In the event that the HR Risk and Compliance team or the data protection authority determine that Skanska or one or more of its employees failed to comply with this policy or any relevant data protection laws, upon recommendation of the authority or HR Risk and Compliance team, Skanska will take appropriate steps to address any adverse effects and to promote future compliance.

19 Policy ownership and responsibility

The owner of this Policy is the Head of Data Protection Compliance who shall ensure that this Policy is properly applied across Skanska supported by the HR Risk and Compliance team.

The Head of Data Protection Compliance is responsible for the oversight and implementation of this policy and may delegate responsibility of communicating policy requirements and any revisions made to this policy to the HR Risk and Compliance team.

20 Monitoring and non-compliance handling

The HR Risk and Compliance team will report breaches of and potential exceptions to this policy to the Head of Data Protection Compliance as soon as possible. Internal audit may also review compliance with this policy and report exceptions to this policy to the Head of Data Protection Compliance, who will escalate such reports to the Skanska Board when appropriate.

21 Policy review cycle

This policy shall be reviewed as required to ensure that the policy is meeting Skanska's purpose. Changes to applicable data protection laws, regulation or regulatory regimes, together with Skanska's risk profile in the global operating environment, may form triggers for revisions or updates to this policy. It is the responsibility of all employees (and supply chain partners) to assist Skanska to comply with this policy.

22 Queries and waivers

Any queries relating to this policy, should (in the first instance) be directed to the HR Risk and Compliance team via the GDPR inbox at gdpr@skanska.co.uk

Any instances where a waiver of this policy is sought must first be reported to the HR Risk and Compliance team and be approved by the Head of Data Protection Compliance.

23 Further information

Refer to the UK Data Protection page for further guidance and supporting documents.