Note that this policy covers both Service Ceilings Limited t/a SCL Interiors & SCL Interiors (London) Limited

Introduction

Purpose

The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, apprentices, and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

The organisation has appointed Hayriye Mazzotta as its data protection officer. Their role is to inform and advise the organisation on its data protection obligations. They can be contacted at Hayriye.mazzotta@sclinteriors.co.uk . Questions about this policy, or requests for further information, should be directed to the data protection officer.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

The organisation processes HR-related personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If the organisation wants to start processing HR-related data for other reasons, individuals will be informed of this before any processing begins.

HR-related data will not be shared with third parties, except as set out in privacy notices. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an

assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in line with our policy on processing special categories of data and criminal records data, which is detailed in Annexe A of this document.

The organisation will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship is held in the individual's personnel file (in electronic format). The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals. The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the UK GDPR.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- Whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- To whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- For how long their personal data is stored (or how that period is decided);
- Their rights to rectification or erasure of data, or to restrict or object to processing;
- Their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- Whether the organisation carries out automated decision-making and the logic involved in any such decision-making.

For more information on how the organisation deals with subject requests, please refer to MSP51 Subject Access Procedure.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful; and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request to info@sclinteriors.co.uk

Data security
The organisation takes the security of HR-related personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. If any of these policies have been breached, the matter will be dealt with under MSP62 Disciplinary Procedure.

Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Computer security:

- Ensuring that firewall and antivirus software is installed on all computers and servers connected to the internet.
- Making sure that operating systems are set up to receive automatic updates
- Protecting computers by downloading the latest patches or security updates, which should cover known vulnerabilities.
- Only allowing staff access to the information they need to do their job and having a policy not to share passwords.
- Encrypting any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Taking regular back-ups of the information on the computer systems and keeping them in a separate place so that information is not lost in the event of a computer failure.
- Securely removing all personal information before disposing of old computers (by using technology or destroying the hard disk).

Other security measures

- Shredding all confidential paper waste
- Physical Security (premises & storage)
- Training staff:
    - So they know what is expected of them;
    - To be wary of people who may try to trick them into giving out personal details so that they can be prosecuted if they deliberately give out personal details without permission.
    - To use strong passwords – these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters, like the asterisk or currency symbols.
    - Not to send offensive emails about other people, their private lives or anything else that could bring the organisation into disrepute.
    - Not to believe emails that appear to come from a bank asking for account, credit or password details (a bank would never ask for this information in this way)
    - Not to open spam (not even to unsubscribe and ask for no more mailings) but to delete the email

Data breaches

If the organisation discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner as soon as possible and in any case not later than 72 hours after discovery. The organisation will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes;
- Not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- Not to store personal data on local drives or on personal devices that are used for work purposes; and
- To report data breaches of which they become aware to the data protection officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

ANNEXE A: Processing Special Category information

Under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, additional protections for job applicants, employees and other data subjects apply if an employer is processing "special categories" of personal data and criminal records data.

This is enshrined within & integral to our data protection policy, and subject to the following definitions, processes & procedures.

Definitions

"Special category personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Why the organisation processes special category personal data and criminal records data

The organisation processes special category personal data and criminal records data for the following purposes.

Equal opportunities monitoring

Data related to racial and ethnic origin, religious and philosophical beliefs, health (including information on whether an individual has a disability) and sexual orientation are processed for equal opportunities monitoring purposes.

Health

Data related to health (including information on whether an individual has a disability) is processed to:

- Ensure that the organisation is complying with its health and safety obligations;
- Assess whether an employee is fit for work;
- Carry out appropriate capability procedures if an employee is not fit for work;
- Ensure that an employee receives sick pay or other benefits to which they may be entitled; and
- Allow the organisation to comply with its duties under the Equality Act 2010 for individuals with a disability.

Racial or ethnic origin

Data related to data subjects' nationality is processed to ensure that the organisation is complying with its obligations to check that they are entitled to work in the UK.

Criminal records data

Criminal records data is processed as part of recruitment processes and, where necessary, in the course of employment to verify that candidates are suitable for employment or continued employment and to comply with legal and regulatory obligations to which the organisation is subject.

Compliance with data protection principles in relation to special category data
The organisation processes HR-related special category personal data and criminal records data in accordance with the following data protection principles.

(1) The organisation processes personal data lawfully, fairly and in a transparent manner and for specified, explicit and legitimate purposes.

Employers can process special category personal data only if they have a legal basis for processing and, in addition, one of the specific processing conditions relating to special category personal data, or criminal records data, applies.

The organisation processes special category personal data and criminal records data for the purposes outlined above and in compliance with the following legal conditions for processing.

Legal basis for processing	**Special category personal data/criminal records data processing condition under sch.1 of the Data Protection Act 2018**
Equal opportunities data	
Processing is in the organisation's legitimate interests. These interests are not outweighed by the interests of data subjects.	Processing is necessary for monitoring equality of opportunity or treatment, as permitted by the Data Protection Act 2018 (under para.8 of sch.1).
Health data	
Processing is necessary for compliance with legal obligations (eg assessing an employee's fitness for work, complying with health and safety obligations, carrying out capability procedures and complying with Equality Act 2010 duties).	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1).
Processing is necessary for the performance of a contract and/or complying with legal obligations (eg administering sick pay and other benefits).	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1).
Racial or ethnic origin data	
Processing is necessary for compliance with legal obligations (eg checking job applicants' and employees' right to work in the UK).	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1).

Criminal records data	
Processing is necessary for compliance with legal obligations (ie the organisation's legal requirement to carry out criminal records checks on those working with children or vulnerable adults). [OR Processing is in the organisation's legitimate interests. These interests are not outweighed by the interests of data subjects. [Use where the organisation is not under a legal obligation to carry out criminal records checks, but it is regulatory good practice to do so.]]	Processing is necessary for the purposes of performing or exercising obligations or rights imposed by law in connection with employment (under para.1 of sch.1). [OR Processing is necessary to comply with regulatory requirements to establish whether someone has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct (under para.12 of sch.1). [Use where the organisation is not under a legal obligation to carry out criminal records checks, but it is regulatory good practice to do so - see below.] OR Processing is necessary for the prevention or detection of unlawful acts (under para.10 of sch.1). [Use where there is no legal obligation to carry out criminal records checks but the organisation can demonstrate that there is a potential risk of unlawful behaviour if they employ someone with a criminal record - see below.]]

The organisation does not use the data for any other purpose and it reviews its processing and policies regularly to ensure that it is not using special category personal data or criminal records data for any other purpose. The organisation will not do anything unlawful with personal data.

Special category personal data and criminal records data are not disclosed to third parties, except in the context of seeking medical advice from the organisation's occupational health adviser or other medical advisers who are subject to a professional duty of confidentiality or reporting suspected offences to the appropriate authorities. The organisation complies with the Access to Medical Reports Act 1988 where relevant.

(2) The organisation processes personal data only where the data is adequate, relevant and limited to what is necessary for the purposes of processing.
The organisation collects and retains the minimum amount of information necessary to allow it to achieve the purposes outlined above.
As noted above, the organisation includes relevant information in privacy notices as to how special category personal data and criminal records data is used and does not use data for any other purpose.
As far as possible, the organisation relies on health questionnaires, rather than medical testing, to obtain necessary information. Any medical testing that is carried out is relevant to the purpose for which it is undertaken and is focused on those performing high-risk roles. It may be a requirement for random alcohol and drug testing to take place due to the high risk activities within the business which are critical to the construction industry.

Criminal records checks are carried out only for individuals undertaking roles where the organisation is under a legal obligation or regulatory requirement to perform such checks or where this is necessary for the prevention or detection of unlawful acts.
All data is reviewed periodically and unnecessary data is deleted.

(3) The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
The organisation takes reasonable steps to ensure that the personal data that it holds is accurate.
Special category personal data and criminal records data is obtained:

- Directly from job applicants, employees and other data subjects; or
- From external sources that the organisation is entitled to assume will provide accurate information, such as the Disclosure and Barring Service in the case of criminal records data, or medical professionals in the case of health data.

The organisation keeps a record of the source of all data it collects and data is reviewed periodically and checked for accuracy. Appropriate records are kept of amendments to data.

The organisation will erase or rectify inaccurate data that it holds without delay in accordance with our MSP27 Data Protection Policy (of which this Annexe is an integral part) if an individual notifies it that their personal data has changed or is otherwise inaccurate, or if it is otherwise found to be inaccurate. Individuals are reminded to review their data on a regular basis to ensure that it remains up to date.

(4) The organisation keeps personal data only for the period necessary for processing.
The organisation has considered how long it needs to retain special category personal data and criminal records data.
It retains and processes special category personal data for [the duration of an individual's employment].
The periods for which special category personal data is retained after the end of employment are as follows:

- Equal opportunities data is kept for a period of six months, after which data is anonymised so that individuals can no longer be identified.
- Health data is normally kept for a period of seven years, unless statutory requirements mean that the organisation must keep records for longer than that.

The organisation does not retain details of an individual's criminal record after the commencement of employment, although it will retain a note on individual HR files indicating that a satisfactory criminal records check was completed prior to the commencement of employment. The note will be deleted at the end of the employment.
At the end of the relevant retention period, the organisation erases or securely destroys special category personal data and criminal records data.

(5) The organisation adopts appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
The organisation takes the security of special category personal data and criminal records data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. The organisation has analysed the risk presented by processing special category personal data and criminal records data and taken this into account in assessing appropriate security requirements. Security levels are set within a

classification register which has helped determine the level of security requirements on Builderstorm and general business information.

Accountability
The organisation has put appropriate technical and organisation measures in place to meet accountability requirements. These include:

- Appointing a data protection officer who reports directly to the organisation's senior management team;
- Maintaining appropriate documentation of processing activities, including special category personal data and criminal records data;
- Adopting and implementing MSP27 Data Protection Policy (of which this Annexe is an integral part), covering HR-related data, which is regularly reviewed

Review and retention of policy and provision to Information Commissioner
This policy on processing special category personal data and criminal records data is reviewed annually and, if necessary, amended to ensure that it remains up to date and accurately reflects the organisation's approach to processing such data.

This policy will be retained by the organisation while special category personal data and criminal records data is being processed and for a period of at least six months after the organisation stops carrying out such processing.

A copy of this policy will be provided on request and free of charge to the Information Commissioner.

Signed: .....

Name: ADAM NURSE

Position: DIRECTOR

Date: 06.09.2023