Data Protection Policy GDPR

January 2021

STREIF

SUSTAINABLE BUILDING SYSTEMS

T 01243 790075 **E** info@streif.co.uk **W** www.streif.co.uk VAT Reg No. 925 4822 16

Company Reg No. 06402905 25 St Pancras, Chichester, West Sussex, PO19 7LT

1.0 Policy Statement

Everyone has rights with regard to how their personal information is handled. During the course of our activities it may be necessary for STREIF UK to collect, store and process personal information about our staff, customers, suppliers and other third parties. The correct and lawful treatment of this data is an essential part of maintaining trustworthy business relationships.

Data users are obliged to comply with this policy when processing personal data on behalf of STREIF UK. Any breach of this policy will be taken seriously and may result in disciplinary action. The Data Protection Legislation applicable in the UK includes provisions for criminal offences for certain mishandling of data.

2.0 Purpose and Scope of Policy

The types of personal data that STREIF UK may be required to handle include information about current, past and prospective suppliers, clients and staff and others that we hold relationships with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Legislation.

This policy and any other documents referred to in it sets out the basis on which STREIF UK will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. This policy does not form part of any employee's contract of employment and may be amended any time. This policy sets out rules on Data Protection and the legal conditions that must be satisfied when we obtain, handle, transfer, store and/or use personal data.

3.0 Definitions of Data Protection Terms

Data is information which is held electronically, or in certain paper based filing systems.

Data Subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal Data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. Personal data does not need to contain the name of an individual to be classified as personal data. The use of a unique identification number (such as an employee number), location data, or an online identifier (such as an IP address) may, in some circumstances, be sufficient to identify an individual.

Data Controllers are the people or organisations that determine the purpose(s) for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies that meet the Data Protection Legislation requirements. STREIF UK is the data controller of all personal data used in its business for its own commercial purposes.

Data Processors include any person or organisation that processes personal data on the instruction of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on a STREIF UK's behalf.

Data Users are those employees (hereafter referred to as those people employed by STREIF UK and those working on STREIF UK premises and where STREIF UK policies are applicable) whose work involves processing personal data. Data users must protect the data they handle in accordance with this policy and any applicable data security procedures at all times.

Data Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to third parties.

Sensitive Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, the use of genetic data or biometric data for the purpose of uniquely identifying individual, physical or mental health or condition or sexual life or sexual orientation, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Data Protection 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 1998 and the General Data Protection Regulation (EU) 2016/679.

Service Provider means any third party company that provides services to STREIF UK.

4.0 Data Protection Principles

Anyone processing personal data must comply with the principles for processing personal data as contained within Data Protection Legislation. These provide that personal data must be:

- Processed fairly, lawfully and transparently;
- Processed for specified, explicit and legitimate purposes and processed in a manner consistent with those explicit purposes;
- Adequate, relevant and limited to the purpose;
- Accurate;
- Not kept longer than necessary for the purpose;
- Processed securely.

Personal data must be processed in a manner that will enable the STREIF UK to demonstrate accountability in meeting each of the six principles.

5.0 Fair, Lawful and Transparent Processing

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly, in a transparent manner and without adversely affecting the rights of the data subject. Data processing must be done in line with data subjects' rights under the Data Protection Legislation.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. These include:

- That the data subject consents to the processing for one or more specific purposes which are made clear to the data subject or;
- That the processing is necessary for:

- The performance of a contract with the data subject (for example an employment contract or a contract for the provision of services) or;
- The compliance with a legal obligation to which the data controller is subject or;
- The compliance with a legal obligation to which the data controller is subject or;
- The legitimate interest of the data controller or another party to whom the data is disclosed (where legitimate interest has been specifically identified and advised to a data subject) and where the processing of data for this legitimate interest does not seriously impact on the interests or fundamental rights of data subjects.

There are other conditions that may be relied on, in limited cases, to permit the processing of personal data. If the processing you are considering does not fall under one of the conditions above, then contact the data protection officer for further guidance.

When sensitive personal data is required to be processed, additional conditions to those set out above must also be met. If you are intending to process sensitive personal data, please contact the data protection officer.

The Data Protection Legislation establishes a requirement to be transparent with the data subject. Where we collect personal data directly from data subjects, we will inform them about the purposes for which we intend to process the personal data, the contact information for the STREIF UK, the details of the data protection officer, the legal basis upon which the processing is reliant (for example consent or a legitimate business interest), details about where the personal data is stored and transfers outside of the UK and/or the European Economic Area, the types of third parties the personal data will be shared with (if any), the period of time the personal data will be stored for, and their rights.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter, but always within one month of having collected the personal data.

We will normally only process sensitive personal data if the data subject has explicitly consented to its processing or there is a legal or regulatory obligation for us to do so. We may also process sensitive personal data where this is necessary for the purposes of equal opportunity and diversity monitoring provided this is carried out with appropriate safeguards for the individuals concerned.

When processing personal data as data controllers in the course of our business, it is important that we ensure that we have met the above requirements as a breach could result in penalties.

6.0 Processing for Specified, Explicit and Legitimate Purposes

In the course of our business, STREIF UK may collect and process personal data that is received directly from a data subject or from other sources. We will only process personal data for legitimate regulatory, client service or

business purposes or for any other purposes specifically permitted by the Data Protection Legislation. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

Personal data may only be processed for the purpose for which it was originally collected. Processing for another purpose to that which was originally specified requires approval from the data protection officer. In considering the use of the personal data for another purpose, the data protection officer should have due regard for whether it is connected with the original purpose, the context in which the personal data was collected, whether it relates to sensitive data and the potential impact on a data subject. Where we process personal data for a different purpose than it was originally collected for, we must notify the data subjects.

7.0 Adequate, Limited and Relevant to the Purpose

STREIF UK will only collect personal data to the extent that it is required for the specific purposes notified to the data subject. You must consider whether the personal data you are requesting a data subject to provide is necessary with a view to minimising the personal data we collect. Furthermore, the personal data should only be accessible by those who need to know, see or process that personal data.

8.0 Accurate Data

STREIF UK will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals thereafter. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Staff are responsible for checking and updating their personal data held by STREIF UK and must immediately notify the company any changes to their personal circumstances.

If requested by a data subject to update, rectify or correct any of that data subject's personal data, that request should be actioned as soon as reasonably practicable, and any service provider which is used to process personal data, shall be informed of the request so that they too can action the request.

9.0 Data Retention

STREIF UK will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. The company will take all reasonable steps to destroy or erase from the data storage systems, all data which is no longer required.

10.0 Data Security

STREIF UK will maintain data security by protecting the confidentiality, integrity and access of personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it;

- Access means that only authorised users (being those who need access to the personal data for a justifiable business reason) should be able to access the data. Personal data should therefore be securely stored on relevant STREIF UK network domain;

Security procedures include:

- Entry controls. Any stranger seen in STREIF UK premises should be challenged;
- Secure lockable physical storage. Pedestals and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential;
- Methods of disposal. Paper documents should be disposed in the confidential waste bins. Digital storage devices should be appropriately wiped when they are no longer required;
- Equipment. Data users must ensure that individual monitors so not show confidential information to passersby and that they lock their computer when it is left unattended.

11.0 Data Subject's Rights Under Data Protection Legislation

STREIF UK will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any data held about them by a data controller (see also clause 15);
- Prevent the processing of their data for direct-marketing purposes;
- Ask to have inaccurate data amended (see also clause 8);
- Object to the processing of their personal data in certain instances;
- Withdraw their consent in the case where consent had previously been granted. Furthermore, we must assess our processing steps where such processing could cause damage or distress and address this appropriately.

12.0 Transferring Personal Data to a Country Outside the EEA

STREIF UK may transfer any personal data we hold to a country outside the European Economic Area (EEA) provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms;
- The data subject has given their consent;
- The transfer is necessary for one of the reasons, or derogations set out in the Data Protection Legislation, such as where it is necessary for the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;
- The transfer is necessary on public interest grounds or for the establishment, exercise or defence of legal claims
- The transfer is authorised by the relevant Data Protection authority where we have confirmed adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms and the exercise of their rights, as may be allowed under Data Protection Legislation.

Subject to the requirements of clause 12.1 above, personal data we hold may also be processed by staff operating outside the EEA that work for us or for one of our service providers. Those staff and/or service providers may be

engaged in, among other things the fulfilment of contracts with the data subject, the processing of payments details and the provision of support services.

13.0 Disclosure and Sharing of Personal Information

Personal data may be shared with STREIF GMBH, so long as this has been notified to the data subject. STREIF UK may also disclose personal data we hold to third parties:

- 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;
- 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.

We may disclose or share personal data if we are under a duty to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property or safety of our employees, customers or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.0 Internal Personal Data Processing

STREIF UK processes personal data relating to its employees and certain employees of service providers. Data users who process personal data on behalf of STREIF UK must process that data in a manner consistent with all relevant clauses in this policy and other applicable STREIF UK policies and those data users are also reminded of their responsibility to maintain the standards contained within this policy as guardians of personal data.

15.0 Internal Personal Data Processing

Data subjects must make a formal request in writing for information we hold about them. Employees who receive a written request for personal data from anyone (whether this is from another STREIF UK employee, a service provider and/or customer) should forward it immediately to the data protection officer.

There is a statutory time period for responding to such requests so it is important that any such request is dealt with promptly as soon as it is received. In responding to a request, where the data subject has not been specific in their request, we should request them to specify exactly what information they want access to. There is no fee for the information request, however, in cases where a request is unfounded or excessive (including repetitive requests), then a reasonable fee (based on the administrative cost) may be charged.

The relevant data controller that has received the request may refuse to provide certain personal data in response to a request from an individual where The Data Protection Legislation provides an exemption. There are very few exemptions for non-disclosure and the application of these exemptions require careful consideration.

When receiving telephone enquiries we will only disclose personal data if that request is followed up by a request in writing. In each case where we are unclear of a requestor's identity, we must request that the data subject provides us with identification documents.

16.0 Implementation, Enforcement and Reporting Data Privacy Incidents

It is very important that we are able to deal with any data security incident as soon as possible to effectively manage the incident. As such, all STREIF UK employees must notify the Data Protection Officer immediately after becoming aware of any data security incident.

A potential data breach is an incident in which sensitive, confidential or otherwise protected data has been accessed, disclosed or handled in a manner inconsistent with the intended treatment of that information. Examples can include unauthorised access of data, loss of data and inappropriate disclosure of data to a recipient.

STREIF UK will require all service providers who process personal data on its behalf to promptly notify us of any potential data security breaches so that we are able to take appropriate action to address the matter.

STREIF UK will provide relevant staff with training about privacy to support compliance with this policy.

STREIF UK will develop, maintain, and publish procedures, guidance and standards to assist achievement of compliance with this policy.

Bill Treves
Managing Director
January 2021