# **Integritypolicy for STICAB Scandinavian Technical Insulation Company AB**. (Order No. 556907-6325 Hereinafter referred to as "**STICAB**"

The purpose of this Privacy Policy is to ensure that STICAB's processing of personal data is made legally and in accordance with the principles of the GDPR. And we handle our customers, employees and suppliers' personal data in a safe and open manner.

## 1. Introduction

In the same way as society as a whole, STICAB, our customers, employees and suppliers have been affected by digitization and globalization, which has led to a significant increase in the use and dissemination of personal data. Digitization means increased opportunities, but also a greater need for protection of the registered personal data and integrity. This policy describes the overall principles that apply to personal data processing within tactics.

### 1.1. purpose

The purpose of this policy is to define STICAB's responsibilities and to identify roles and responsibilities for compliance with the Data Protection Ordinance (GDPR).

### 1.2. Goal

The objective is that STICAB's processing of personal data is legally valid and in accordance with the principles of GDPR to ensure that our customers, employees and suppliers are handling our personal information in a safe and transparent way.

### 1.3. definitions

This policy uses the following definitions:

**Personuppgiftsansvarig**

The natural or legal person, public authority, agency or other body, alone or jointly with others, determines the purpose and method of processing personal data.

**Personuppgiftslämnare**

The living person to which the personal data applies. A personal information provider is defined in this policy as a person such as Tactics has some kind of relationship with, for example, customer, employee, consultant or other.

**Personal Data Assistants**

A natural or legal person, public authority, institution or other person who processes personal data for the personal data controller.

personal Information

Any information that is directly or indirectly attributable to a natural person is in the personal data act as personal data. Even images (photos) and sound recordings on individuals treated by computer can be personal data even if no names are mentioned. Encrypted data and various types of electronic identities, such as IP numbers, are counted as personal data if they can be linked to natural persons.

**Privacy policy**

All forms of personal data processing include personal data processing, such as collection, registration, organization, structure, storage, processing, alteration, production, reading, use, disclosure, dissemination or provision by other means, adjustment or assembly, restriction, erasure or destruction.

**1.4. Extent**

The scope of this policy is limited to personal data processing as required by the General Data Protection Ordinance (GDPR). This includes STICAB, external consultants who perform tasks on behalf of STICAB and Personal Data Advisers who perform data processing on behalf of STICAB.

In addition to the general guidelines in this policy, detailed requirements of local data protection laws, where applicable, must be followed by employees in the processing of personal data.

In the case of STICABs, personal data counsel for an external organization, data processing shall be done in accordance with this policy, unless otherwise specified in a personal data grant agreement between STICAB and the person responsible.

**1.5. Target groups**

The privacy policy applies to all personnel performing tasks on behalf of STICAB regarding the processing of personal data. It is also intended as the basis for information to personal information providers regarding personal data processing. This also applies to personal data advisors who perform personal data on behalf of STICAB.

**2. Roles and Responsibilities**

Below we describe roles.

### 2.1. CEO

The CEO shall ensure that STICAB is properly organized with delegated responsibility and sufficient resources for processing personal data within the company and is ultimately responsible. CEO is reached via mikael.nilsson@sticab.se

### 2.2. HR

Human resource manager is responsible for identifying information security risks for staff, customers and suppliers as well as suggesting appropriate information control and monitoring of information security controls. HR is available via mikael.nilsson@sticab.se

### 2.3. Personuppgiftsansvarig

Personal Data Responsibility is always responsible for processing personal data. Personal Data Responsibility is always the legal person who controls and decides on the handling of personal data.

### 2.4. Responsible for Personal Data / Privacy Officer (PO)

The role of the role is to ensure the provision of GDPR in its organization. This is also required to keep a record of all processes that include personal data carried out by organization. PO is reached via mikael.nilsson@sticab.se

### 2.5. Personal Data Assistants

External IT service providers, cloud services and the like where personal data are processed on behalf of STICAB are called personal data assistants. A personal data commissioner shall perform the tasks specified in a personal data grant agreement.

### 2.6. Employees

All employees are personally responsible for the legal and correct processing of personal data in their daily work. By following STICAB's governing personal data handling documents, employees contribute to compliance with proper personal data processing.

## 3. Data protection requirements

Below we describe how personal data and data protection are handled.

### 3.1. Legal basis for processing

Personal data may only be processed if certain conditions are met, for example (A) if the person to which the personal data relates has given consent to the treatment. (B) The processing is necessary for the performance of a contract to which he is a party. (C) The processing is necessary for STICAB to comply with a legal obligation. or (D) STICAB's legitimate interest in processing personal data outweighs the individual's interest in not receiving their personal data.

### 3.2. Principles for processing personal data

Legality, Correctness and Transparency - When processing personal data within STICAB, we shall ensure that the processing is legal and that we are transparent to personal data providers.

Data Minimization - Within STICAB, we never collect and handle more personal data than is required to fulfill the purpose of the data. This means that we need to ask ourselves in each collection of personal data if necessary. If the purpose of data processing has expired, we must remove personal data that is no longer required.

Objective Limitation - When collecting personal information, we must have a clear and legitimate purpose in collecting and processing. If the purpose is no longer valid, we must remove the personal data processed accordingly. If we want to process personal data for a new purpose, it should not be incompatible with the original purpose, for example, beyond what the person-related person concerned would reasonably expect. We must also ensure that the personal data provider is informed of this, and for which legal basis we process personal data.

Accuracy - Personal information must be accurate and current. Personal information that is incorrect or incomplete should be deleted or corrected.

Storage minimization - Personal data will only be stored for as long as necessary for the purposes for which the data is processed or as required by applicable law. When that time has elapsed, personal data must be permanently deleted in a safe manner. If we want to keep personal data for a longer period than is necessary for the purpose, we must ensure that the data can no longer be linked to a person, directly or indirectly (anonymization). For personal data we received from a person we have a customer relationship with, we retain these during the period of time that constitutes a practice determined by the National Data Protection Authority.

Integrity and Confidentiality - The personal data must be protected, including against unauthorized or unauthorized treatment and against loss, destruction or accidental injury. STICAB should therefore take appropriate technical and organizational measures to protect personal data.

Disclaimer - STICAB is responsible for compliance with the principles of personal data processing when processing personal data and to show how they are followed.

### 3.3. Personal Data Provider's Rights

STICAB shall respond to the wishes of the Personal Data Provider in the manner required by applicable law or otherwise deemed to be reasonably practicable and appropriate in consultation with our PO.

Transparency and information - Persons whose personal data are processed should be informed in a clear manner. Such a message should be concise, easily accessible, written in clear and simple language, and must contain certain specific information.

Right to information - An individual may request information about STICAB's processing of personal data.

Right to rectification and deletion - An individual may request that personal data be corrected or deleted.

Right to object - In some cases, an individual is entitled to object to the processing of his or her personal data by the person responsible.

Right to object - Applies to the processing of personal data to perform a task of public interest, as part of the exercise of authority or after a balance of interest.

An individual is entitled to complain against STICAB's processing of his / her Personal Data.

An individual is entitled to compensation for damage

### . 3.4. Personal Data Responsible and the Personal Data Commissioner's duties

When processing is carried out by a personal data commissioner on behalf of the data controller, personal data administrators shall only use personal data advisors who can provide sufficient guarantees for implementing adequate technical and organizational protection to meet the requirements of GDPR and thus protect the personal data provider

There must be a legally binding agreement between the Data Protection Officer and the Personal Data Commissioner meeting the requirements of data protection laws and the distribution of responsibilities made between the parties regarding personal data processing:

Data protection through privacy by design - Any new service or business process introduced by STICAB involving personal data processing should be designed to take into account the protection of such data, for example, by ensuring that the necessary security measures are built into its design ("privacy by design"). Any such new service or business process shall also be designed to ensure that by default only

personal data necessary for the specific purpose of the processing are treated ("privacy by default").

Impact assessment of data protection - Where there is a high risk of personal data processing, especially when it comes to new technologies, cloud services and other IT systems, STICAB should conduct an impact assessment before such processing. STICAB will then follow the data inspection guidelines on impact assessment.

Reporting of Personal Data Incidents - Employees who suspect that this policy or relevant data protection laws have been violated should contact STICAB PO immediately to enable STICAB to comply with statutory notification requirements.

Provision of the Personal Data Provider's Rights - as set out in Chapter 3.2 of this Policy.

Security measures - An employee who has access to personal data may only process the data in accordance with the purpose of the processing and may not share, distribute or otherwise disclose the personal data to a third party unless instructed to do so by STICAB. Appropriate technical and organizational measures should be implemented to protect personal data against accidental or illegal destruction, accidental data loss or alteration, unauthorized disclosure or access and other illegal forms of processing. Appropriate safeguards in relation to the risk should be taken.

The transfer of personal data outside the EU and the EEA is only allowed when the importing entity has provided sufficient guarantees that personal data will be adequately protected. This can be achieved by using one of the EU's standardized data transfer agreements. Contact PO for further information.

Education and awareness - STICAB provides adequate education for all employees, based on employee role and responsibility.

## 4. Personal data management at STICAB

Below we describe our personal data management.

### 4.1. Personal data where STICAB is the person responsible for personal data

#### 4.1.1 Information on our corporate customers

In order to fulfill the agreement with customer, contact details are recorded, such as invoice and delivery address. These data are recorded in our business system and are processed for billing and accounting purposes.

#### 4.1.2. Suppliers & Subcontractors

Because we purchase some services that we may need, personal data will also be treated as a supplier or subcontractor. This is because we can make payments or contact you in one way or another so that you can effectively perform your mission or offer your product or service.

This applies to the following categories of registered:

**- Employee of a supplier company**

**- trainees**

**- Consultants**

### 4.1.3. Potential employees

We also process data as we receive job applications.

### 4.2. What we use your personal information to

When processing your personal data, we do so with your consent and / or on a need basis, in order to drive our business, comply with our contractual and legal obligations, protect our systems or meet other legitimate interests, primarily related to sales and marketing activities.

### 4.2.1. Carry out obligations as a contractor

In order for STICAB to fulfill its obligations as a contractor and to ensure safe and efficient administration, it is necessary for STICAB to collect, process and store personal data at freelancers, consultants and other subcontractors. Only personal data related to the assignment are processed.

### 4.2.2. Customer support

We use data to provide support and support services for you to take advantage of our Services.

### 4.3. Types of personal data we process and for what purposes

We do not use data for purposes other than those described in this policy. The data we process may include the following:

### 4.3.1. Name and contact details

We collect first and last name, e-mail address, mailing address, phone number, delivery details and other similar contact information. These data are processed to enable us to fulfill agreements and commitments with our customers, partners and staff.

### 4.3.2. Personal identification number and payment information

In order to meet our agreements with suppliers, subcontractors, customers and partners, we need to collect payment information. Note that personal identification numbers are only registered with staff so that we can register and pay agreed compensation and report them to the Swedish Tax Agency.

#### 4.3.3. Device and usage data

It may also include operating system information, including IP address, device ID, national settings, and language settings.

#### 4.3.4. Film and Photo

Participation in corporate presentations, customer assignments and the like is done only with consent and involvement of co-workers, such as social media and the

company's website.

#### 4.3.5. Support and feedback

We also collect information that you provide us and the content of messages you send to us, such as feedback or questions and information you provide for customer support.

#### 4.3.6. Sensitive personal data

We usually do not deal with sensitive information, except for a few interview situations where the content itself may be of a sensitive nature.

### 4.4. What your personal information may be shared with and why we share them

In cases where we share information about you with others, we have determined that these companies comply with our data protection requirements and are not allowed to use personal data they receive for any purpose other than agreed.

### 4.5. Systems and cloud suppliers

It may sometimes be necessary for us to share your information with external companies to facilitate our business, deliver our services, and fulfill our obligations. For example, it may be about system and cloud suppliers we use to bring our work forward. However, these can not be viewed without our explicit permission.

### 4.6. Email and other unstructured data

STICAB has a special internal policy for processing personal data in e-mail and other unstructured data. Firstly, we need a legal basis for managing email. STICAB, like other companies and private organizations, can usually process personal information in incoming e-mail based on a balance of interest. The policy also states that STICAB should not use e-mail to systematically handle personal data, as well as discoloration.

### 4.7. Other

Finally, we may need to disclose or save your information when we consider it necessary to:

- Follow the law or legal process and provide information to the police and other competent authorities.

- Protect our customers, for example, to prevent spam or fraud, or to facilitate the prevention of death or serious injury.

- Manage and maintain the security of our services, including preventing or stopping an attack on our systems or networks.

- Protecting rights or property belonging to STICAB, including enforcing the terms governing the use of the services, but if we get information that someone uses our services to trade stolen intellectual or physical property belonging to STICAB, we will not investigate a customer's own private content, but we can then transfer the matter to a police authority.

### 5. Contact us

If you have any questions about your personal data, request for a registry, a complaint or a question to our PO, please contact us at mikael.nilsson@sticab.se. We answer questions within 20 days.

### 6. Internal audit

STICAB will make objective internal audits of this policy, including data protection on periodic basis. The CEO of STICAB is responsible for overall monitoring and implementation of this policy. The CEO is responsible for STICAB's daily compliance with this policy and data protection laws.

Stockholm 2018-05-15

Mikael Nilsson

Managing Director