Privacy is important to us, this Policy provides information about the data we collect, process and share and it demonstrates our commitment to always using the personal data we collect in a respectful manner.

Policy prepared by:	Rachel Power, O'Dwyer Power, in consultation with Management
Controller:	STS Group Companies
Address:	Block 10A, Cleaboy Business Park, Old Kilmeaden Road, Waterford
Contact:	Email: info@stsgroup.ie Phone: +353 (0)51 508009
Privacy Coordinator:	Bernadette Morrissey
Approved by Management on:	01/07/2018
Policy became operational on:	01/07/2018
Policy reviewed on:	21/01/2021
Next review date:	21/07/2021

Privacy Policy Overview

STS Group needs to gather and use certain information about individuals. This Policy applies to personal information we obtain from individuals through our website, in providing our services and as an employer. A copy of our Privacy Policy is made available to our customers on request. We may update this Policy at any time we deem appropriate to reflect any changes in our services.

This policy applies to:

- All companies within the STS Group:
  - Specialist Technical Engineering Services Unlimited Company
  - STS Group Switzerland AG
  - STS Elektromechanische Anlagenbau GmbH
  - STS Specialist Technical Services UK Ltd
  - Specialist Technicial Services Sweden AB
  - STS Buhindi W.L.L
  - Specialist Technical Engineering Services B.V
  - STS D&V Group
- The offices and site offices of STS Group
- All staff and volunteers of STS Group
- All contractors, suppliers and other people working on behalf of STS Group

Under Data Protection Law, we at STS Group are deemed a controller. As a controller we guarantee the privacy and security of our own employee's personal information as well as that of our customers.

Data Protection Law

The Regulation (EU) 2016/679 (General Data Protection Regulation), hereto referred to as GDPR, effective as of 25th May 2018, which replaced the Directive 95/46/EC, describes how businesses must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Regulation is underpinned by important principles. These say that personal data must:

- Be processed fairly and lawfully;
- Be obtained only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the purpose for which it was originally collected;
- Be adequate, relevant and not excessive;
- Be accurate and kept up to date;
- Kept in a form that permits identification of data subjects for no longer than necessary; and
- Processed in a manner that ensure appropriate security of the personal data.

A controller (in this case, STS Group) is responsible for being able to demonstrate compliance with the GDPR and the above principles.

Individuals have certain basic rights under the GDPR, including:

- The right to have personal information processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- The right to be informed, this means that STS Group needs to tell you what data we are using, why we are using it and for what purpose as well as informing you of the details of any third parties in receipt of data from us;
- The right of access, you are allowed to see what data of yours we are processing if you request that from us;
- The right of rectification, that means if the data we are using is incorrect we must correct it;
- The right to erasure (or right to be forgotten), this means that you have the right to issue a request to us requesting the erasure of your personal data. However, in certain cases, there will be overriding legitimate grounds for continued processing and we may be unable to comply with such a request;
- The right to restrict processing, this means that you can ask you to stop using your data unless we have a legitimate lawful purpose for continuing to do so;
- The right to data portability, this means that you have the right to move your data to another data processor and we must provide you with a copy of your data “in a structured, commonly used and machine-readable format”;
- The right to object, this means that you can object to the use of your data and we must stop using it unless we have an over-riding legitimate reason to continue;
- The right not to be subject to automated decision making, including profiling;
- The right to make a complaint to the Supervisory Authority (in Ireland this is the Data Protection Commissioner); and
- The right to judicial remedy.

Why We Collect Information and Data?

We rely on various information to run our business, this information may include data that could be used to identify an individual. This is referred to as personal data or personal information. Part of the purpose of this Policy is to give examples of how personal data is collected and why it is used. For example, when a customer enlists our services to tender for a project, we require basic personal information in order to communicate with them and maintain a working relationship.

We also collect information to perform our obligations as an employer and to properly carry out the administration of our staff in area such as training.

Some of the services that require the processing of personal data include:

- Design, co-ordination and planning services to provide mechanical and electrical solutions;
- Specialised procurement to develop and deliver supply chain strategies for projects;
- Mechanical and electrical services to produce fully engineered, quality designs of all sizes;
- Project construction including data centres, pharmaceutical and the utilities sector;
- Industrial facility commissioning; and
- Maintenance of key mechanical and electrical systems.

What Types of Personal Data Do We Collect?

The following examples are indicative of the type of personal data that we may collect, the exact type of data will depend on the services being used:

- Contact information (such as name, email address, home address, phone numbers)
- Financial information (such as taxation details, income, bank details)
- Identification data (such as PPS number, date of birth, fingerprint, facial image)
- Employment details (such as occupation)
- IP Addresses (via our website)

How Do We Collect Personal Information?

There are a few ways we collect personal information. We collect information directly from you (via email or over the phone or in person) when you initially engage our services. As part of a recruitment process, we will collect information about candidates through such mediums as email, post, Facebook or in person.

You decide on how much information to share with us, however, refusing to share certain information may limit our ability to provide you with the services you require.

We collect information about our employees when they take up employment with us and throughout the course of their employment in the performance of their duties and on-going development.

How Do We Use Personal Information?

We use your personal information for such purposes as:

- To assess candidates who apply for positions in our company as part of a recruitment process;
- To compile tenders for services with prospective customers;
- To provide you with the services you request;
- To maintain a working relationship;
- To order supplies or engage third party services;
- To bill you for our services; and
- Under our contractual obligations as an employer.

The personal data we collect from you is directly relevant to our services and obligations.

What Is Our Lawful Basis For Processing Personal Information?

As defined in the Regulation, we are required to demonstrate our legal basis for processing Personal Information.

When you engage our company to provide you with a service, we are relying on Article 6(1(b)) GDPR which states “processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”. This is also the basis for processing carried out under our obligations as an employer.

We also rely on the lawful basis of “legitimate interests”. in order to carry out a recruitment process. We must communicate with candidates and collect certain personal information in order to assess their suitability to the position being applied for considering them for future positions.

When we send you information relating to a service you have enquired about, or are submitting a tender for a specific project, we are relying on Article 6(1(f)) GDPR which states “processing is necessary for the purposes of the legitimate interests pursued by the controller”.

When Do We Share Personal Information?

We do not sell your personal information, nor do we share it with unaffiliated third parties unless we are required to do so by law. We may disclose your personal information to third parties so as to provide you with our services, or with quotes for our services, to facilitate a change to our business, as required by law, when engaging third parties under a contractual agreement for professional services or with your consent.

We may share personal information in some of the following ways:

- With a third party processor in the performance of their duties under a contractual agreement and under which they are bound by confidentiality;
- With certain representative bodies in the construction industry such as the CIF (Construction Industry Federation) for purposes of registration or administration;
- To engage professional services of specialist third parties, any such parties are bound by confidentiality;
- In connection with a tender for a project where certain personal information is required for the purposes of securing the contract for the project, all parties are bound by confidentiality in these cases;
- The law may require us to share information, but we will only share information that is necessary to satisfy requirements;
- We reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal;

- In connection with, or during negotiations of a business merger or sale or similar business transfer provided that such party agrees to use such Personal Information in a manner consistent with this Policy;
- To ensure the security of our IT systems in order to protect your data.

We do not share your Personal Information with third parties for their own marketing use without your express permission.

We may share information between the companies in the STS Group, which may include transfers of data both within the EU and outside the EU. In cases where data is shared between the STS Group companies, this processing is carried out as per Recital 48 GDPR which states that Controllers that are part of a group have a legitimate interest in transferring data within the group to third countries.

What Security Measures Do We Have?

We use administrative, organisational, technical and physical securities to protect the Personal Information we collect and process. We ensure that we adopt appropriate controls which guarantee the security and confidentiality of your Personal Information.

For personal Information gathered in paper form:

- When not required, documents or files are kept in a locked drawer or filing cabinet;
- Staff are instructed to make sure paper and printouts are not left where unauthorised people could see them, like on a printer;
- All offices containing paper files containing Personal Information are locked when left unattended for any long period of time;
- Only authorised personnel are permitted to access confidential Personal Information; and
- Data printouts are shredded and disposed of securely when no longer required.

When data is stored electronically, it is protected from unauthorised access, accidental deletion and malicious hacking attempts. We adopt the following controls:

- Staff are instructed to use strong passwords that are changed regularly and never shared between staff;
- When working with personal data, staff are instructed to ensure the screens of their computers are always locked when left unattended;
- Staff are instructed to always double check an email address prior to sending information via email;
- If data is stored on removeable media (e.g. Memory stick) these are kept locked away securely when not being used and are protected appropriately in case lost or stolen;
- Staff are instructed not to remove any data or documentation from our offices unless this is required specifically for external project work, meetings or the performance of their duties;
  Staff are instructed to always keep information strictly confidential and not to disclose or discuss an employee's or customer's information or circumstances with any unauthorised outside parties;
- Data is only stored on designated drives and only uploaded to approved IT systems;
- Staff do not save copies of personal data to their own computers and instead, always access and update the central copy of any data;
- Cloud Backups are done daily and stored securely off-site;

- Data is never saved directly to laptops, PC hard drives or other mobile devices like tablets or smart phones; and
- All computers containing data are protected by approved security software and a firewall.

When data is processed by a third-party processor it is done so under a contractual agreement, we ensure that the processor uses appropriate technical and organisation measures to guarantee the security of the data we send to them.

Responsibilities

Everyone who works for or with STS Group has some responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data is instructed to ensure that it is handled and processed in line with this policy and data protection principles.

The Board are ultimately responsible for ensuring that STS Group meets its legal obligations and abides by its own policies and procedures. The company's Privacy Coordinator is responsible for handing any Data Protection queries from both internal and external individuals as well as ensuring any new staff are aware of their responsibilities and for promoting awareness of Data Protection within the company.

Data Protection responsibilities include:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- Ensuring regular security checks are carried out to guarantee hardware and software is functioning properly;
- Approving any data protection statements attached to communications such as emails and letters;
- Addressing any data protection queries from data subjects, reviewing documentation annually and arranging training for any new members of staff as required;
- Recording any subject access requests (SARs) from individuals to see the data STS Group holds about them and following the SAR procedure;
- Ensuring that any Data Processing Agreements with third parties are adequate and are in place where required;
- Ensuring any breaches are recorded in the internal breach register and reported to the Data Protection Commissioner in line the company's Data Breach Procedure; and
- Ensuring any new staff receive a copy of the Employee Privacy Policy.

Data Accuracy

The law requires STS Group to take reasonable steps to ensure data is accurate and kept up to date. The more important it is that the personal data is accurate, the greater effort we put into ensuring its accuracy.

It is the responsibility of all staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as possible;
- We will update the Personal Information we hold on your direct instruction at any time;

- Data is updated as inaccuracies are discovered.

Subject access requests (SARs)

All individuals who are the subject of personal data held by us are entitled to:

- Ask what information the company holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date;
- Be informed how the company is meeting its data protection obligations.

SARs from individuals should be made by email, addressed to the data controller at info@stsgroup.ie. We will then supply a SAR request form which will assist us in responding to a request. However, individuals are not obliged to complete this form in order for us to comply with the request. We will respond within one month to any request subject to proof of identity.

Prior to complying with a SAR, we require proof of the applicant's identity and address to ensure that the person making this access request is acting legitimately, failure to provide us with adequate proof of identity will regrettably result in the SAR being denied.

Data Retention

Retention periods depend on different criteria, including compliance with legislation and best practice. The following is our current schedule for retention of information, we may revise or update this schedule at any time we deem appropriate.

Personal information for all general enquiries	3 years
Emails	Emails will be retained for 5 years
Customer details obtained for Projects	10 years from cessation of relationship
Personal Information from job applicants	1 year
Subject Access Requests	3 years
Breach Reports	3 years
Data Processing Agreements	3 years from cessation of relationship
IT contracts	6 years
Minutes of Board meetings	6 years

Note: Our Employee Privacy Policy contains retention periods for staff records.

Privacy at STS Group

At all times STS Group will take your privacy seriously and not infringe on your rights regarding the processing of your personal data. If at any stage you have concerns about your personal data, please contact our Privacy Coordinator by emailing info@stsgroup.ie.

Signed:  **Date: 22/07/2020**

Richard Hogan
Managing Director
Specialist Technical Services