



## Personal Records, Confidentiality and Data Protection Policy

The following Data Protection policies and practices are in line with the General Data Protection Regulations (GDPR) 2018.

All employees must notify Stainless UK Ltd of their permanent home address, telephone number, next of kin, bank branch, and account number. It is important that changes in personal circumstances are notified immediately to management. These include changes to the following:

- Name
- Address / telephone number
- Dependants (e.g., for private medical insurance purposes)
- Beneficiaries (e.g., for death in service benefit)
- Persons to be notified in case of emergency
- Bank details for salary payments
- Tax code


All employees are also reminded that the nature of their work means that they will become party to information that is of a sensitive and confidential nature. In particular, employees are reminded that they should not discuss any aspect of any client's affairs or matters outside work and must not become involved in gossip involving clients whilst in work as such conversations can be overheard and could result in a serious breach of privacy and confidentiality which could affect the relationship with the client.

Some employee records are kept on computer. In accordance with the provisions of Data Protection legislation, employees may request a printout of the information held on computer. The information held by Stainless UK Ltd about employees will be made available to the employee on request, together with a description of the purposes for which the company keeps this information, and to whom it may be disclosed. Periodically, employees will be asked to check the data held by the company. Stainless UK Ltd is under an obligation to comply with the Data Protection legislation. The full GDPR policy statement is set out below.

### **GDPR Privacy Standard**

#### **Introduction**

1. This Privacy Standard sets out how Stainless UK Ltd handles the personal data of our customers, suppliers, employees, workers, and other third parties.
2. This Privacy Standard applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other data subject.

<b>Signed</b>	<b>Print</b>	<b>Title</b>	<b>Date</b>	<b>Page</b>
	<b>Tim Wells</b>	<b>Managing Director</b>	<b>09/01/2025</b>	<b>1 of 8</b>



## Personal Records, Confidentiality and Data Protection Policy

This Privacy Standard applies to all company personnel. Employees must read, understand, and comply with this Privacy Standard when processing personal data on behalf of Stainless UK Ltd and attend training on its requirements. This Privacy Standard sets out what is expected from employees in order for the company to comply with applicable law. Compliance with this Privacy Standard is mandatory. Any breach of this Privacy Standard may result in disciplinary action.

**Scope** Stainless UK Ltd recognises that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.


The company is responsible for overseeing this Privacy Standard. Please contact a Director with any questions about the operation of this Privacy Standard or the GDPR, or if you have any concerns that this Privacy Standard is not being or has not been followed.

In particular, employees must always contact a Director in the following circumstances:

- If unsure of the lawful basis which is being relied on to process personal data
- If needing to rely on consent and/or need to capture explicit consent
- If unsure about the retention period for the personal data being processed
- If unsure about what security or other measures need to be implemented to protect personal data
- If there has been a personal data breach
- If needing any assistance dealing with any rights invoked by a data subject
- If needing help complying with applicable law when carrying out direct marketing activities
- If needing help with any contracts or other areas in relation to sharing personal data with third parties

**Personal Data Protection Principle** Stainless UK Ltd adheres to the principles relating to the processing of personal data set out in the GDPR, which require personal data to be:

- Processed lawfully, fairly, and in a transparent manner (lawfulness, fairness, and transparency)
- Collected only for specified, explicit, and legitimate purposes (purpose limitation)
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (data minimisation)
- Accurate and, where necessary, kept up to date (accuracy)
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (storage limitation)

Signed	Print	Title	Date	Page
	Tim Wells	Managing Director	09/01/2025	2 of 8



## Personal Records, Confidentiality and Data Protection Policy

- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage (security, integrity, and confidentiality)
- Not transferred to another country without appropriate safeguards being in place (transfer limitation)
- Made available to data subjects, allowing them to exercise certain rights in relation to their personal data (data subject's rights and requests)

Stainless UK Ltd is responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).


**Lawfulness, Fairness, Transparency** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject. Stainless UK Ltd may only collect, process, and share personal data fairly and lawfully and for specified purposes. The GDPR restricts actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that personal data is processed fairly and without adversely affecting the data subject.

The GDPR allows processing for specific purposes, some of which are set out below:

- The data subject has given their consent
- The processing is necessary for the performance of a contract with the data subject
- To meet legal compliance obligations
- To protect the data subject's vital interests
- To pursue legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects

The purposes for which Stainless UK Ltd processes personal data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices. The company must identify and document the legal ground being relied on for each processing activity.

**Consent** A data controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent. A data subject consents to the processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action, so silence, pre-ticked boxes, or inactivity are unlikely to be sufficient. If consent is given in a document that deals with other matters, then the consent must be kept separate from those other matters.

Signed	Print	Title	Date	Page
	Tim Wells	Managing Director	09/01/2025	3 of 8



## Personal Records, Confidentiality and Data Protection Policy

Where explicit consent is required, Stainless UK Ltd must issue a fair processing notice to the data subject to capture explicit consent. The company will need to evidence consent captured and keep records of all consent so that it can demonstrate compliance with consent requirements.

**Transparency (notifying data subjects)** The GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices, which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.


Whenever Stainless UK Ltd collects personal data directly from data subjects, including for human resources or employment purposes, it must provide the data subject with all the information required by the GDPR, including the identity of the data controller and DPO, how and why the company will use, process, disclose, protect, and retain that personal data through a Fair Processing Notice, which must be presented when the data subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publicly available source), Stainless UK Ltd must provide the data subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. The company must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates the proposed processing of that personal data.

**Purpose Limitation** Personal data must be collected only for specified, explicit, and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. Stainless UK Ltd cannot use personal data for new, different, or incompatible purposes from that disclosed when it was first obtained unless the company has informed the data subject of the new purposes, and they have consented where necessary.

**Data Minimisation** Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties. You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes. You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

**Accuracy** Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You will ensure that the personal data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular

Signed	Print	Title	Date	Page
	Tim Wells	Managing Director	09/01/2025	4 of 8



## Personal Records, Confidentiality and Data Protection Policy

intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.


**Storage Limitation** Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. You must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements. The Company will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held unless a law requires such data to be kept for a minimum time. You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Company’s applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable. You will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

**Security, Integrity, and Confidentiality Protecting Personal Data** Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage. We will develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

You are responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure. You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it
- Integrity means that personal data is accurate and suitable for the purpose for which it is processed

Signed	Print	Title	Date	Page
	Tim Wells	Managing Director	09/01/2025	5 of 8



## Personal Records, Confidentiality and Data Protection Policy

- Availability means that authorised users are able to access the personal data when they need it for authorised purposes

You must comply with and not attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

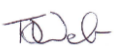
**Reporting a Personal Data Breach** The GDPR requires data controllers to notify any personal data breach to the applicable regulatory and, in certain instances, the data subject. We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for personal data breaches. You should preserve all evidence relating to the potential personal data breach.

**Transfer Limitation** The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit, send, view or access that data in or to a different country. You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms
- Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO
- The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks
- The transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest

**Data Subjects' Rights and Requests** Data subjects have rights when it comes to how Stainless UK Ltd handles their personal data. These include rights to:

- Withdraw consent to processing at any time
- Receive certain information about the data controller's processing activities

Signed	Print	Title	Date	Page
	Tim Wells	Managing Director	09/01/2025	6 of 8



## Personal Records, Confidentiality and Data Protection Policy


- Request access to their personal data that Stainless UK Ltd holds
- Prevent Stainless UK Ltd.'s use of their personal data for direct marketing purposes
- Ask Stainless UK Ltd to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- Restrict processing in specific circumstances
- Challenge processing which has been justified on the basis of Stainless UK Ltd's legitimate interests or in the public interest
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format

Stainless UK Ltd must verify the identity of an individual requesting data under any of the rights listed above. Stainless UK Ltd must immediately forward any data subject request received to the line manager.

**Accountability** The data controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles. Stainless UK Ltd have adequate resources and controls in place to ensure and to document GDPR compliance.

**Record Keeping** The GDPR requires Stainless UK Ltd to keep full and accurate records of all data processing activities. These records should include, at a minimum, the name and contact details of the data controller, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period, and a description of the security measures in place. To create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

**Training and Audit** Stainless UK Ltd is required to ensure all personnel have undergone adequate training to enable them to comply with data privacy laws. Stainless UK Ltd must also regularly test systems and processes to assess compliance. All systems and processes under control must be regularly reviewed to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

Signed	Print	Title	Date	Page
	Tim Wells	Managing Director	09/01/2025	7 of 8



## Personal Records, Confidentiality and Data Protection Policy


**Direct Marketing** Stainless UK Ltd is subject to certain rules and privacy laws when marketing to customers. For example, a data subject’s prior consent is required for electronic direct marketing (for example, by email, text, or automated calls). The limited exception for existing customers known as “soft opt-in” allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message. The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject’s objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

**Sharing Personal Data** Generally, Stainless UK Ltd is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. Personal data may only be shared with another employee, agent, or representative of the group (which includes subsidiaries and the ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions. Personal data may only be shared with third parties, such as service providers if:

- They have a need to know the information for the purposes of providing the contracted services
- Sharing the personal data complies with the Privacy Notice provided to the data subject and, if required, the data subject’s consent has been obtained
- The third party has agreed to comply with the required data security standards, policies, and procedures and put adequate security measures in place
- The transfer complies with any applicable cross-border transfer restrictions
- A fully executed written contract that contains GDPR-approved third-party clauses has been obtained

**Failure to Comply** Failure to comply with this policy could lead to disciplinary action potentially resulting in summary dismissal.

**Changes to this Privacy Standard** Stainless UK Ltd reserves the right to change this Privacy Standard at any time without notice, so please check back regularly to obtain the latest copy of this Privacy Standard.

Signed	Print	Title	Date	Page
	Tim Wells	Managing Director	09/01/2025	8 of 8