Stannah
An independent family business since 1867

Stannah

Group Policy Statement

General Data Protection Regulation (GDPR)

Issue date: March 2018 **Number: 5982399** **Issue: 01**

Responsibility: GMT

Scope

All Stannah companies conducting business in Europe.

Purpose

This policy sets out how we seek to protect personal data and ensure that employees understand the rules governing the use of personal data set out in the General Data Protection Regulation and the Data Protection Act 1998 (as replaced by the 2018 Act). This policy requires employees to consult with their relevant Steering team member before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

This policy is supplemented by the Use of Computers & Technology policy and IT Governance procedure.

The GMT has overall responsibility for this policy, with a data protection team representing each operating company having responsibility for the day-to-day implementation.

Definitions

- Data Subject: A data subject is the living individuals to whom the data relates.
- Personal Data: Any information relating to an identifiable living person (the data subject) who can be directly or indirectly identified, particularly by reference to an identifier.
- Special Category Data: (sensitive data) The special categories of Personal Data specifically include data relating to ethnicity, religion, union membership, health, sex life, genetic data, and biometric data where processed to uniquely identify an individual.
- Data Controller: A controller determines the purposes and means of processing personal data.
- Data Processor: A processor is responsible for processing personal data on behalf of a controller (this can be the same legal entity or a third party).
- Supervisory Authority: Within the UK this is the Information Commissioners Office

Policy

The Principles

Lawfulness, Fairness and Transparency - Personal Data must be Processed lawfully, fairly and in a transparent manner.

Purpose Limitation - Personal Data must be collected only for specified, explicit and legitimate purposes.

Data Minimisation - Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which it is Processed.

Accuracy - Personal Data must be accurate and kept up to date.

Storage Limitation - Personal Data must not be kept for longer than is necessary to carry out the purposes for which the data was collected.

Security, Integrity and Confidentiality - Personal Data must be 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.

Transfer Limitation -Personal Data must not be transferred to another country without appropriate safeguards being in place.

Data Subject's Rights and Requests - Personal Data must be made available to Data Subjects. Data Subjects must be allowed to exercise certain rights in relation to their Personal Data.

Accountability - We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

Lawfulness, Fairness and Transparency

Personal data must be processed fairly and lawfully in accordance with Data Subjects' rights. This generally means Personal Data should not be processed unless there is a legal basis to allow it. For Stannah the lawful basis is one of the following

- Legal requirement
- Contract
- Legitimate Interest
- Consent

Privacy Notice - transparency of data protection

We publish and maintain a privacy notice to data subjects.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees.
- Highlights that we may be required to give information to third parties such as expert witnesses and other professional advisers.
- Identifies that data subjects have certain rights over the data that we hold about them.

We strive for transparency in providing accessible information to individuals about the use of their personal data.

Conditions for processing

We ensure any use of personal data is justified using at least one of the conditions for processing and this is specifically documented. All employees who are responsible for processing personal data are aware of the conditions for processing. The conditions for processing are available to data subjects in the form of a privacy notice.

Sensitive personal data

In most cases where we process sensitive personal data, it requires the data subject's explicit consent to do this unless exceptional circumstances apply (such as in the field of employment where no consent is needed), or we are required to do this by law (e.g. to comply with legal obligations to ensure health and

safety at work). Any such consent clearly identifies what the relevant data is, why it is being processed and to whom it will be disclosed. Consent should be clearly recorded and refreshed at appropriate intervals.

Consent

Unless there is a legitimate reason to collect data in order to fulfil a legal obligation in connection with employment or otherwise to protect the vital interests of the Data Subject or it is necessary for legal proceedings, sensitive personal data is only collected with explicit active consent by the data subject. This consent can be revoked at any time.

Purpose Limitation

We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this, or would otherwise reasonably expect this.

Data Minimisation

Privacy by design and default

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. All system projects, involving personal data, have a requirement for a Privacy Impact Assessment. We have procedures to ensure that employees understand their responsibilities

Accuracy

Accuracy and relevance

We ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

Individuals may ask for any inaccurate personal data relating to them to be corrected.

Your personal data

Employees must take reasonable steps to ensure that personal data held is accurate and updated as required. For example, if personal circumstances change, the employee can self-manage their Ofbiz HR record.

Storage Limitation

Data retention

Personal data is retained for no longer than the purpose it was originally obtained for. The retention period is defined on the data register. It is then deleted or securely archived

Security, Integrity and Confidentiality

Details are covered in the IT Governance procedure

Transfer Limitation

Transferring data internationally

Personal Data may be transferred outside of the EEA only where suitable protection is provided and one of the following conditions applies:

(i) 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. Please speak to the Data Protection Team to confirm which countries these are.

(ii) appropriate safeguards are in place such as binding corporate rules, 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 Data Protection Team;

(iii) the Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

(iv) 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, in some limited cases, for our legitimate interest.

These rules are complicated and non-compliance can result in large fines. If your professional duties require you to transfer Personal Data outside of the EEA, you must not do so without first speaking to the Data Protection Team.

Post-Brexit, the UK will still have to maintain these high standards to ensure that it becomes one of the countries listed in (i) above.

Data Subject's Rights and Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- Withdraw of Consent to Processing at any time.
- Receive certain information about the Data Controller's Processing activities.
- Request access to their Personal Data that we hold.
- Prevent our use of their Personal Data for direct marketing purposes.
- Ask us 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 our legitimate interests or in the public interest.
- Object to decisions based solely on Automated Processing, including profiling.
- Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.
- Be notified of a Personal Data Breach only 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.

You must immediately forward any Data Subject request you receive to the Company Data Protection Team. You should promptly assist him/her with the Data Subject request if asked to do so.

We must verify: (i) the identity of an individual requesting data under any of the rights listed above and (ii) any authorisation from the data subject if the request is being made by a third party on their behalf. Do not allow third parties to persuade you into disclosing Personal Data without proper authorisation as this will put The Stannah Group in breach of these laws.

Subject access requests

Upon request, a data subject has the right to receive a copy of their personal data in a structured format. Subject access requests must be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.
When a 'subject access request' is received, the employee should refer the request immediately to the Data Protection Team.

Employees can access their information in Ofbiz and should contact HR if they have any concerns. Please note that there are restrictions on the information to which the employee is entitled to under applicable law.

Right to be forgotten

A data subject may, in limited circumstances, request that any information held on them is deleted or removed. This is a limited right and is weighed up against the company's legitimate interests to continue processing. If granted, the deletion of personal data must flow down to any third parties who process or use that personal data and they must also comply with the request. An erasure request can be refused if an exemption applies or the right does not exist due to circumstances in processing.

The Rights of Individuals to object to Direct Marketing

Employees should abide by any request from an individual not to use their personal data for direct marketing or profiling purposes and notify the Data Protection Team [and marketing team] about any such request.

Direct marketing material should not be sent to someone electronically (e.g. via email) unless they have given consent. This consent must be valid under GDPR and must be refreshed when appropriate.

Please contact the Data Protection Team for advice on direct marketing before starting any new direct marketing activity.

Criminal record checks

We will conduct criminal record checks only when this is permitted by law. Criminal record checks do not necessarily require the consent of the subject.

Accountability

Data audit and register

Regular data audits to manage and mitigate risk are performed and the Data Register updated. The Data Register contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All employees have an obligation to report actual or potential data protection compliance failures to the Data Protection Team. This allows Stannah to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures, where these failures create a risk to the individual data subjects.
- Notify individuals if the breach causes a high risk to them

Full details for managing a Data Breach is published in the IT Governance procedure.

Training

Employees in relevant roles receive suitable training on this policy. Training is refreshed periodically or if there is a substantial change in the law, policy or procedures.

Training covers:

- The law relating to data protection
- Stannah's data protection and related policies and procedures.

The completion of training is compulsory for all relevant employees.

Responsibilities of Data protection team.

- Keeping the GMT updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection training and advice for all employees and those included in this policy.
- Answering questions on data protection from employees, board members and other stakeholders.
- Responding to individuals such as customers and employees who wish to exercise their rights under GDPR.
- Checking and approving data processing contracts or agreements for suppliers / contractors who handle the company's data.

The data protection team comprises of representatives of the Stannah Group companies.

Consequences of failing to comply

Stannah takes compliance with this policy very seriously. Failure to comply puts the business and employees alike at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under Disciplinary Procedure, which may result in dismissal.

If you have any questions or concerns about this policy, please do not hesitate to contact the Data Protection Team.