Thomas Tait & Sons Limited 1988 Pension Scheme - Data Protection Policy

Introduction

The Thomas Tait & Sons Limited 1988 Pension Scheme ("the Scheme") is fully committed to full compliance with the requirements of the EU General Data Protection Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (GDPR) which applies from 25 May 2018. The Scheme will follow procedures which aim to ensure that all Trustees, administrators, service providers and advisers (collectively known as data users) who have access to any personal data held by or on behalf of the Scheme are fully aware of and abide by their duties under the GDPR.

The Scheme is registered with the Information Commissioner's Office (ICO) under registration number Z935625, this registration having commenced on 24 October 2001 and currently expiring on 23 October 2023. The Scheme will continue to maintain its registration with the UK ICO as part of its obligations to continue to comply with the GDPR.

This Data Protection Policy should be read in conjunction with:

- the Cyber Security Policy; and
- the Scheme's Privacy Notice.

Statement of Policy

The Trustees need to collect and use information about members and beneficiaries to operate and carry out their functions. This personal information must be handled and dealt with properly; however, it is collected, recorded, used and erased and whether it is on paper, in computer records or recorded by other means.

The Trustees regard the lawful and appropriate treatment of personal information as vital to the operation of the Scheme.

This Policy forms a part of the Trustees' obligations to demonstrate accountability.

Controller

The Trustees recognise that they are a controller for the purpose of the GDPR particularly in regard to members and beneficiaries. As such, the Trustees are responsible for compliance with the GDPR and for overseeing those who process data on the Trustees' behalf. Those who process data on the Trustees' behalf are known as its processors.

The Trustees understand that, for some purposes, some of their suppliers and professional advisers, including the Scheme's actuary, legal adviser and auditors will be also be controllers.

Processors

The Trustees' processors include the Scheme's administrators and other service providers who are not themselves controllers. The Trustees will ensure that their processors have provided suitable guarantees about their compliance with the GDPR and have entered into an agreement with the Trustees that meets the requirements of the GDPR.

Basis for processing personal information

The Trustees will usually process personal information because it is necessary for compliance with their legal obligations and/or because they have a legitimate interest to do so (which are both lawful bases under the GDPR). This is because the data is required for the administration of the Scheme. In particular, it is required to calculate and pay benefits, to advise members about their options and to deal with any queries that members have. It is also needed to ensure that the Scheme operates efficiently and provides accurate information to members.

Sometimes, the Trustees may rely on other grounds for processing personal information, such as it being necessary to comply with contractual obligations.

Occasionally, information may be processed on the basis that the members have consented to this, for example where information relates to 'special category data' such as health data.

In the case of 'special category data' processing may also take place without consent where this is permitted by the GDPR. For example, such processing may take place where processing is necessary for the purpose of the establishment, exercise or defence of a legal claim.

Alternatively, under the Data Protection Act 2018, the processing of 'special category data' and information relating to criminal convictions (if these relate to money owed to the employer) without consent is permitted when exercising obligations or rights under employment, social security or social protection laws, for the purpose of assessing working capacity or for medical diagnosis. The Trustees will rely on whichever of these two conditions applies in respect of Special Categories Data and data relating to criminal convictions already held by the Scheme even if at the time the data was collected the data subject was asked to give consent.

Where the two above conditions do not apply, express consent to the processing of 'special category data' is needed.

Where consent is relied upon, it must be explicitly given and not implied. Members will be told about their right to withdraw their consent at any time and the Trustees will facilitate any withdrawal of consent. As consent must be specific, the Trustees will generally take professional advice before seeking consent from members, to ensure that the consent is properly given. The Trustees will also generally take professional advice before processing 'special category data' without consent or before processing information relating to criminal convictions. Information about this is set out in the privacy notice.

Handling Personal/Sensitive Data

The Trustees will, through management and use of appropriate controls, monitoring and review:

- Use personal data in the most efficient and effective way in order to operate the Scheme under current legislation and the Trust Deed and Rules;
- Provide guidance and training for Trustees and Scheme administrators at an appropriate level;
- Strive to collect and process only the data or information which is needed;
- Make appropriate arrangements if provided with more data or information than is needed;
- Use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted;
- Strive to ensure information is accurate;
- Not keep information for longer than is necessary (although recognising that pensions are long-term obligations);
- Securely destroy data which is no longer needed;
- Take appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data);
- Ensure that any data breaches are dealt with appropriately;
- Ensure that information is not transferred abroad without suitable safeguards;
- Ensure that there is general information available to members and beneficiaries of their rights to access information;
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR.

These rights include:

- The right to access their own personal information within one month of the request;
- The right to correct, rectify, block or erase information regarded as wrong information;
- The right to have personal information deleted and to object to processing.
- to receive privacy notices;
- to restrict processing of personal data;
- to receive a copy of their personal data or transfer their personal data to another data controller;
- to object to processing of personal data;
- not to be subject to automated decision-making; and
- to receive notification of a Scheme Personal Data Breach where it is likely to result in a high risk to the rights and freedoms of the Data Subject, or where required to do so by the ICO.

The Trustees note their responsibility to provide any communication, or take any actions, requested by a Data Subject in exercise of the rights referenced above, free of charge, except on the rare occasion where such requests are unfounded or excessive.

Data Security Measures

To ensure that data security is maintained, the following policies and procedures will be followed:

- Where paper documents continue to be held, those not in current use will be stored and locked securely.
- Any personal data/member records that are not in current use or otherwise stored will be locked away outside of normal working hours.
- The presence of paper documents will be minimised as far as possible through retaining them electronically.
- Any copy documentation that is surplus to requirements is confidentially disposed of via a shredding process, or otherwise dealt with by a similar method.

<u>Electronic Storage of the Scheme's own data</u>

All of the Scheme owned data that is stored on the local server is subject to the standard security, back up and disaster recovery procedures and checks that the Scheme's Administrators operate to.

Email Policy

Wherever possible, the use of email to transfer personal member data will be avoided by using relevant adviser secure upload web-based portals.

Whenever the transfer of personal member data by email is unavoidable, all such data files are password protected and the password separately advised to the recipient. Furthermore, wherever possible, unnecessary details identifying the member concerned will be redacted from such data prior to transfer. Where possible, personal data should be transferred by encrypted means.

Transfers of data outside the EEA

The Trustees will seek to ensure that data is not transferred outside the EEA without appropriate safeguards being in place. Where the data is transferred to a non-EU Commission approved country, appropriate contractual safeguards will be required.

Professional advice will be taken if it is proposed that personal information be transferred outside the EEA directly by the Trustees. Transfers outside the EEA may be made by the Trustees' processors where this is permitted by their agreement with the Trustees.

Retention of personal information

The Trustees recognise that personal information should only be retained for so long as necessary.

Where a person retires on a pension under the Scheme, the Trustees believes that it is necessary to retain their personal information until the member's (and in the case of a spouse's pension until that spouse's) death. If a pension death benefit becomes payable, the information will be retained until that pension ceases. Once there is no further liability, the information will be kept indefinitely in case any future claims are made.

Where a member transfers out of the Scheme or takes all benefits as a cash sum, the member's personal information will be kept indefinitely in case any future claims are made.
The Trustees believes that retaining personal information for this length of time is in line with its obligations, legitimate interests and the interests of the Scheme as a whole and is also in the interests of the people concerned. This is because it is important to be able to demonstrate that benefits have been paid correctly and that the Scheme has discharged its liabilities and to be able to deal with any queries raised about this in the future.

Maximum Data Storage Periods

Individual Trustees must not retain Scheme documentation on their personal PC once the individual case has been determined (personal member data) or beyond a period of four years (non-personal data).

When hard copy documents are held by individual Trustees they will be securely locked away or held at an RTSL location, and confidentially disposed of once the individual case has been determined (personal member data) or after four years (non-personal data).

Individual Trustees should destroy Scheme hard copy documents in accordance with the storage period policy noted above. Documents should be confidentially disposed of, through the document shredding process at an RTSL location.

Trustee Director Compliance with the GDPR

Upon appointment, any new Trustee Director will be required to confirm via his/her appointment letter, that they will comply with the GDPR.

At Trustees' meetings:

- There will be a standing agenda item requesting confirmation from the Directors present whether they are following the Scheme's data protection policy
- All agenda items will be categorised as to whether they contain personal member data or not – such classification being an indicator to the Directors as to the maximum storage period for the related papers (this requirement to apply at sub-committee meetings also)

External Electronic Storage of Scheme Documentation

From time to time, the Directors may decide to have Trustee meeting and other key documentation hosted on an external website in to simplify the distribution of such papers in advance of meetings (and avoid their dissemination via email). The Directors will ensure that appropriate security and access controls exist around such third-party sites.

Scheme Website

The Trustees may decide to make available their own website for scheme members. Such a website may contain Scheme generic data (such as member booklets and newsletters), but will not contain any personal member data.

Links to other websites may be included on the Scheme's website, such as where members will be able to access information regarding their own pension investments. However, access to members' own data will be controlled by those other third-party service providers, such as on their own websites.

Relationships with Third Parties

The Trustees will ensure that third parties providing services to the Scheme have incorporated appropriate GDPR compliance statements into their contractual arrangements with the Scheme and will seek confirmation on an annual basis that they maintain, and will continue to implement and maintain, appropriate cyber security safeguards in line with regulatory and industry guidance, considering the nature and scope of the service they provide to the Trustees.

The Trustees also receives confirmation that the Scheme Administrator has cyber security protections in place.

Fair Processing Notice

The Trustees will make available a privacy notice to Scheme members. The privacy notice will set out:

- the Trustees' contact details;
- the purposes of the processing and the legal basis for this;

- the categories of data held;
- the recipients or categories of recipients of the data;
- information about transferring data outside the EU and of the safeguards in place;
- details of the period for which data will be retained;
- the existence of the right to access data and of the right to have it rectified or erased;
- the right to withdraw consent (where consent is being relied upon);
- the right to complain to the ICO;
- details of where the data originates from if collected from a third party.

The Trustees will usually review the privacy notice on an annual basis and will review it before undertaking any new processing activity. If necessary, an updated notice, or other form of communication, will be issued before any new processing activity is carried out.

Data mapping and Records of processing activities

The Trustees will maintain a written record of its processing activities as controller. This will set out:

- the Trustees' name and contact details and those of any joint controller;
- the purpose of the processing;
- the categories of data subjects and the categories of personal data;
- the categories of recipients to whom data has been or will be disclosed;
- details about transfers of data outside the EEA, including the name of the recipient country, and of the safeguards in place;
- the time limit for retention of the data;
- a general description of the technical and organisational security measures;
- information relating to the conditions under which special category data and information relating to criminal convictions is processed.

The Trustees' processors must maintain similar records.

Dealing with breaches of the GDPR

The Trustees recognise that breaches of the GDPR can have serious consequences and must be dealt with quickly.

If a breach is considered serious, the Trustees will be notified immediately. If there is uncertainty as to whether a breach is serious, the Trustees will consult to determine whether the breach should be reported.

Professional advice will be sought about how to deal with the breach and whether the Information Commissioner's Office (ICO) and the members concerned need to be notified.

Notification to the ICO is required without delay (and in any event within 72 hours) unless the breach is unlikely to result in a risk to the member concerned. Members must be notified without undue delay where the breach causes a high risk to them.

Those who process data on behalf of the Trustees are required to notify the Trustees of any breach without undue delay after becoming aware of it.

Data protection impact assessments

If the Trustees believe that a new form of processing will carry a high risk, for example if it uses new technologies, an impact assessment may be carried out.

However, in many cases, the Trustees expect that its processors will have carried out assessments in those circumstances as to the level of risk involved.

Data Protection Officer

The Trustees have been advised that it is not legally required to appoint a data protection officer ("DPO"). This is because a DPO is only required where: (1) the core processing activities consist of regular and systematic monitoring of data subjects on a large scale or (2) where processing of health data on a large scale occurs on a large scale, and the Trustees undertake neither type of processing.

Review of Policy

The Trustees shall carry out a regular review of the decisions set out in this Policy and, when necessary and with regard to any supplementary guidance introduced by the ICO, issue a revised policy.

The Trustees shall ensure that the Policy and its compliance with the GDPR are reviewed each time a new third-party adviser is appointed to provide services to the Scheme, or in the event that a new system is adopted.

The Trustees shall also carry out a regular review of any other relevant documentation, including any data sharing agreements in place. To assist with the Trustees' regular review of this Policy, it will be noted on the Trustees' risk register and Scheme calendar.

The Trustees reserve the right to amend this Policy from time to time.

Data Protection Contact Details

Scheme administrators: edinburgh-ops@mercer.com

Trustees: info@rosstrustees.com

Appendix 1: The Principles of Data Protection

The GDPR stipulates that anyone processing personal data must comply with 6 principles of good practice. These principles are legally enforceable.

In summary, the principles require that personal data:

1. Shall be processed lawfully, fairly and in a transparent manner;
2. Shall be obtained only for specified, explicit and legitimate purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in a manner that ensures appropriate security of the personal data;

The GDPR provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data is defined as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data or biometric data for the purpose of uniquely identifying a natural person
- Physical or mental health or condition;
- Sexual life or sexual orientation.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.