THE WORSHIPFUL COMPANY OF ACTUARIES

and

COMPANY OF ACTUARIES CHARITABLE TRUST

Data Protection Policy

April 2018

Contents

This policy covers the following:

1. Background

In the course of running its day to day business and promoting its charitable and educational aims, The Worshipful Company of Actuaries (the '**Company**'), may collect and process information about its members and staff as well as members of the public such as enquirers and correspondents. The use of such information ('**personal data',** as explained in more detail below) is regulated by data protection law (the '**Data Protection Legislation**', explained below). This policy sets out how the Company intends to comply with the key rules that apply to the processing of personal data in the United Kingdom.

This policy document also covers the activities of the Company of Actuaries Charitable Trust, which holds the same data as the Company and is supplied by the Company.

Description of the Company's processing activities

The Company regularly processes the following categories of personal data:

Staff: The Company has no employees,

Members: The Company holds the personal data of its past, present and prospective members (Liverymen, Freemen, Honorary Freemen and Companions). The personal data held is documented in the Appendix to this document. The Company processes such personal data in order to administer membership, to organise events such as meetings and social events, and to collect subscription fees. It also processes members' personal data for fundraising purposes including seeking endowments such as gifts, trusts and bequests. The Company holds some information about its members for archival and historical research purposes, for example, to maintain a roll of past Freemen and Liverymen.

Beneficiaries: The Company's charitable and educational activities have been a fundamental objective throughout its history. In order to further its charitable and educational aims, the Company may process personal data about beneficiaries and potential beneficiaries, which may include personal, family and financial circumstances, education, and employment history. The Company may occasionally process information about beneficiaries' or prospective beneficiaries' health or medical details. The Company may also process personal data about its beneficiaries for historical and archiving purposes.

The public: The Company may enter into correspondence with members of the public, such as enquirers, correspondents. When it does so, the Company may collect incidental personal data such as contact details and personal circumstances, and processes such personal data in order to respond to queries and deal with ad hoc issues.

Suppliers: The Company processes personal data concerning its suppliers of goods and services, including identifiers such as contact details, financial information and purchase history. The Company processes such information in order to purchase goods and services, to pay its suppliers and to maintain its accounts and records. .

This policy does not document every part of the Data Protection Legislation which may be relevant, but merely focuses on the key aspects that are likely to be applicable to the Company. Should other issues arise in practice not covered by this policy, the Company will consider these separately at the time. The Company will review this policy annually, and may amend it from time to time as it sees fit.

2. Applicable data protection law

Data protection law in England and Wales is primarily found in the Data Protection Act 1998 ('**DPA**'). With effect from 25th May 2018, the DPA will be repealed and superseded by the General Data Protection Regulation ('**GDPR**'). The GDPR will be supplemented by the Data Protection Act 2017. In this policy, any reference to the Data Protection Legislation means the DPA, or the GDPR, as supplemented by the Data Protection Act 2017 ('**DPA 17**'), whichever is in force at the time.

The DPA is enforced in England by the Information Commissioner, operating through the Information Commissioner's Office (the '**ICO**'). The ICO publishes guidance on the DPA and has a broad range of powers, including the ability to issue fines of up to £500,000 for breaches. The ICO will enforce the GDPR when it takes effect in May 2018. Under the GDPR, the ICO will have greater powers, including the ability to issue fines of up to 4% of annual turnover, or €20,000,000, (whichever is greater) and to conduct compulsory audits of organisations' data handling practices.

3. Key concepts of applicable data protection law

The Data Protection Legislation relies on a number of key definitions, which are explained below.

'***personal data***' means any information relating to an identified or identifiable natural person (a 'data subject', which is explained in more detail below). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the identity of that natural person.

The Company will hold personal data about its past, present and prospective members (including Liverymen and Freemen) staff and members of the public such as beneficiaries, as well as its suppliers. The Company may hold such personal data both in electronic and hard copy format, in records, correspondence and minutes.

'***processing***' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

organisation, structuring, storage, adaption or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing is interpreted very broadly, so that almost all activities organisations carry out in relation to their personal data are captured by the definition.

The Company will generally be deemed to be processing any personal data that it may collect, record, store and/or disclose.

'***controller***' means the natural or legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data. The Data Protection Legislation applies to controllers, who must comply with its requirements.

The Company will generally be a controller in relation to the personal data of its members, staff, members of the public such as beneficiaries and enquirers, and suppliers.

'***processor***' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Where a controller uses a processor to process personal data on its behalf, the controller must only use a processor that provides sufficient guarantees to ensure that personal data is processed securely, and in accordance with the requirements of the GDPR. **The Data Processor will normally be the Clerk to the Company**.

The Company may use processors for a variety of purposes; for instance, to store personal data, or to send email communications. In each case, it must have conducted sufficient due diligence to be able to evaluate whether the processor offers sufficient guarantees to protect personal data and must ensure that the processor is bound by a contract that incorporates the provisions specified by the GDPR. The requirements around appointing processors are explained in more detail below (see Section 7, below).

'***special categories of personal data***' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data, data concerning health (including medical data, and medical records, for example), or concerning an individual's sex life or sexual orientation. Special categories of personal data is the term used in the GDPR which, broadly speaking, replaces the concept of 'sensitive personal data' from the DPA.

The special categories of personal data require a higher standard of care. If a personal data breach (as defined below) occurs that involves the loss of any of the special categories of personal data, the ICO will regard this as a serious breach. The GDPR also requires that personal data relating to criminal convictions and offences is treated with a higher standard of care.

The Company is very unlikely to hold the special categories of personal data, though in the event that it does, it must ensure the information is handled accordingly.

'***data subject***' means an individual to whom personal data relate. Typically, these are employees, customers, and suppliers.

The categories of data subject whose personal data the Company is likely to process will include members, staff, suppliers and members of the public.

'***personal data breach'*** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach may be accidental, such as a system failure, or loss of an electronic or physical file, or malicious, such as a cyberattack. In the event that the Company suffers a personal data breach, it must take specific steps, explained below in this policy.

4. The data protection principles

The data protection principles are standards which the Company must observe when processing personal data. These principles are as follows:

i. Fairness, lawfulness and transparency

This is the most important of the data protection principles and comprises three elements; fairness, lawfulness and transparency. Considering these in more detail:

Fairness: Organisations generally cannot process individuals' personal data in a way that an individual would not have reasonably expected. Collecting personal data on the pretext of one purpose and then using it for another, unrelated purpose is unlikely to be fair. The Company should consider whether its uses of personal data would fall within the reasonable expectations of the affected data subjects.

Transparency: Organisations must provide certain prescribed information to individuals when processing their personal data, including the organisation's identity, the purposes for which personal data are being processed, or are to be processed, and any third party recipients of the personal data. A complete list of the information that must be provided to data subjects can be found in Articles 13 and 14 of the GDPR. The transparency information must accurately reflect the controller's use of personal data. This is frequently provided by way of a website privacy notice, but may also be provided by way of a disclaimer on a paper form, or a pre-recorded message in the context of recorded telephone calls.

The Company must ensure that its website privacy notice, and any other means by which it makes the transparency information available to data subjects (such as a disclaimer on a paper form) accurately and comprehensively reflect its processing activities.

Lawfulness: Organisations must establish at least one of a number of lawful grounds for processing. These lawful grounds are set out in Article 6 of the GDPR and are as follows:

1) The data subject has given his or her **consent** to the processing. Note that to be valid, consent must be freely-given, informed (by way of the transparency notice, explained above) specific, and capable of withdrawal at any time, without detriment to the data subject. Consent must be indicated by way of an unambiguous, positive affirmation by the data subject. Consent cannot be inferred from the absence of an objection, and will not be valid where the data subject does not have a genuine choice.

2) Processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.

3) Processing is necessary for **compliance with a legal obligation** to which the controller is subject.

4) Processing is necessary in order to protect the **vital interests of the data subject** or of another person.

5) Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.

6) Processing is necessary for the purposes of **legitimate interests** pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.

In practice, the Company will frequently be able to rely on the second and sixth grounds (performance of a contract, and the legitimate interests ground) for many of its activities. Note that the grounds for processing the special categories of personal data are different.

ii. Purpose limitation

This principle requires that the purposes for which personal data are processed are limited to those purposes specified in the transparency information that has been provided to the affected data subjects, and not processed for any further, incompatible purposes. Note that any further processing operations for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible purposes.

The Company should only process personal data it holds for those purposes specified in the website privacy notice, or other such transparency notice.

iii. Data minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Company should only collect the personal data that is strictly necessary for the purpose for which it was collected, and should not collect additional, unnecessary personal data on a 'just in case' basis.

iv. Accuracy

Personal data must be kept accurate, and up to date.

The Company must ensure that any requests from data subjects to update their personal data are dealt with promptly, having satisfied itself as to the requester's identity.

v. Storage limitation

Personal data must not be kept for longer than is necessary for the purposes for which the data are processed. The duration for which personal data are stored will be dictated by applicable legal, business or other reasons, such as retention periods driven by tax legislation.

If the Company cannot establish a valid legal, business or other reason for retaining personal data, it should be securely deleted. The Company should specify the periods for which personal data are stored in a record retention policy. After the storage period has expired, personal data should be deleted.

Note that the Company may store some categories of personal data for longer periods where such processing is solely for archiving purposes in the public interest, or historical research purposes. In such cases, the Company must implement appropriate safeguards, such as allowing data subjects to request deletion of some of their personal data.

vi. Integrity and confidentiality

Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Company should take appropriate measures that are proportionate to the risk associated with the personal data it holds. Such measures may be technical, such as encryption and password protection of electronic devices and electronic storage media (e.g. USB drives), or organisational, for example, by operating a layered access policy, appropriate vetting of staff who have access to personal data, conducting appropriate due diligence on any third parties that process personal data on the Company's behalf, and binding them by an appropriate engagement contract. The Company should consider regularly reviewing and testing its security measures.

vii. Accountability

Controllers are responsible for compliance with the principles explained above, and must be able to demonstrate compliance.

The Company must be in a position of being able to provide evidence of compliance, for example, by way of a data protection policy, documented data protection reviews and a record of data protection training.

5. Data subjects' rights

Data Protection Legislation confers a number of rights upon data subjects, which controllers must observe. Data subjects' rights are a cornerstone of The Data Protection Legislation, and must be dealt with promptly should one arise. The Company is unlikely to receive data subject requests on a regular basis so this Policy does not go into detail but the Company must be able to recognise a request from a data subject to exercise his or her rights, should one arise. The most relevant of these rights, from the Company's perspective, are summarised below:

i. Data subject access requests

Data subjects are entitled to access their personal data held by the Company on request (Article 15 GDPR). The response to a data subject access request must include certain information, such as: the purposes of the processing; the recipients (or categories of recipient) to whom the personal data have or will be disclosed; and individuals' rights to have their data corrected, deleted or to restrict the processing of their data.

Note that under the GDPR, the information must be provided to data subjects free of charge and within one month of the request. This differs from the previous position, under the DPA, which allowed the Company to charge a fee of up to £10 for dealing with a request, and the response period was 40 days.

ii. The right to be forgotten

Data subjects have the right to request the Company to erase all data held in respect of them in various circumstances (Article 17 GDPR). However, the right to be forgotten is not an absolute right, and the Company is only obliged to give effect to a request in a number of specific situations, the most relevant of which are likely to be:

1) Where the purpose for which the personal data were processed no longer applies; or

2) Where the Company's processing of the personal data is based on consent and the data subject withdraws his or her consent.

iii. The right to rectification

Data subjects have the right to have incorrect personal data about them corrected without undue delay (Article 16 GDPR).

The Company must endeavour to ensure that any personal data it processes is up to date and correct. Where an error or inaccuracy is discovered, the Company should correct this as soon as possible.

iv. The right to data portability

Data subjects have the right, in certain circumstances, to access their data in machine-readable format and, where technically possible, to have their data transferred directly from the Company to another data controller (Article 20 GDPR). However, the circumstances in which the right to data portability arises are limited and, at present, seem unlikely to be relevant to the Company.

v. The right to object

Data subjects have the right, in a number of specific circumstances, to object to having their personal data processed (Article 21 GDPR). The most relevant of these circumstances are where the processing is based on the Company's legitimate interests (explained in section 4(i)(6) above. Data subjects may also object to their personal data being processed by the Company for direct marketing purposes.

6. Other requirements

The Company must process personal data in accordance with the principles explained above. However, the Data Protection Legislation imposes a number of additional requirements, which are explained below.

i. Breach notification

The ICO would expect the Company to have a documented data protection breach management plan in place. In the event of a data protection breach, the ICO would regard the absence of a breach management plan as an aggravating factor.

Reporting breaches to the ICO

Under the GDPR, if a data security breach occurs, the Company (as controller) must notify the breach to the ICO "*without undue delay" and, where feasible, within 72hrs of the personal data breach occurring*." However, this notification requirement does not apply where the breach "*is unlikely to result in a risk to the rights and freedoms*" of the individuals concerned.

The notification must include the information specified in Article 33(3) of the GDPR, and where it is not possible to provide all the information at once, it may be provided in phases.

Reporting breaches to individuals

Where a data security breach occurs, and it is likely to result in a "high risk" to the rights and freedoms of the individuals concerned, the Company must notify the affected individuals *"without undue delay".* Article 34(2) of the GDPR specifies what information must be provided. However, the Company is not required to notify data subjects if:

1) The personal data concerned had been rendered unintelligible (for example, by way of encryption); or

2) Subsequent measures have been taken by the Company so that there is no longer a high risk to the individuals; or

3) It would involve disproportionate effect to communicate to each affected data subject individually, although where this applies then a general public communication must be made.

The Company must maintain a schedule of data breaches (whether or not notification was made at the time), to comply with Article 33(5) of the GDPR.

ii. Data protection impact assessments (DPIAs)

A DPIA consists of a documented consideration and evaluation of the data protection risks arising from a proposed new processing activity, along with recommended mitigation strategies to address the risks.

Under Article 35 of the GDPR, the Company is required to undertake a DPIA "*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*"

The Company does not believe that the nature of its processing is such that there is likely to be a high risk to the rights and freedoms of the data subjects whose personal data it

holds. As a result, the Company does not believe that it is necessary for it to undertake any DPIAs.

The Company will keep this conclusion under review, including any guidance issued from ICO, or practice in other similar schemes

7. Third party processors

The rules around the appointment of processors (the meaning of which is explained in Section 3, above) are strict, and amount to an organisational security measure. In the event that the Company were to suffer a personal data breach involving a third party processor, the ICO would expect to see that appropriate due diligence had been conducted on that provider and that the appropriate contract was in place.

Before the GDPR comes into force, the Company must ensure that it has a written contract which meets the requirements of GDPR in place with each processor it uses. The Company must only use processors that guarantee they will meet the requirements of the GDPR and will protect data subjects' rights.

Before engaging a processor, the Company will check that the processor has appropriate technical and organisational measures in place to keep data secure; and that the processor's staff who will be engaged in processing personal data on behalf of the Company are subject to a duty of confidentiality and receive regular training in data protection matters.

The Company should regularly review the activities and processes of any processors it uses, to check that the processor is processing personal data in line with its internal processes; complying with relevant requirements under the Data Protection Legislation and its contractual commitments in respect of the personal data. The Company will ensure that its contract with each processor contains provisions concerning sub-contracting which meet the requirements of GDPR.

8. Further information

For further information about this policy, and the Company's data handling practices or for a data subject access request, please contact:

Mr Lyndon Jones
clerk@actuariescompany.co.uk
The Clerk
Actuaries' Company
Cheapside House
138 Cheapside
London
EC2V 6BW

Appendix

Data handling process and practice

Data held

The following data is held on every member and prospective member who has applied to become a member of the Company:

Name
Partner's name
Address
Telephone numbers
Preferred email address
Employer
Date of birth
Year qualified as an actuary
Year of entry into Company membership
Membership number
Bank account details

The data (other than bank details) is managed by the Clerk and is held in a password protected Excel spreadsheet. The password is changed regularly.

Bank account details are held in paper form by

- the member of the Finance Committee responsible, from time to time, with collecting Quarterage by direct debit; and
- the Almoner of the Charitable Trust who deals with donations made by standing order.

Users of data

A copy of the database is kept by the:

Clerk - for the day to day operation of the Company
Secretariat – for the purpose of communicating with members, on the request of the Clerk
Honorary Treasurer – for the purpose of processing membership fees
Chairman of the Membership Committee – for verifying proposers and seconders
Member of the Finance Committee dealing with Quarterage by direct debit
Almoner and Assistant Almoner of the Charitable Trust – for the purpose of operating the charitable trust

From time to time, the database is made available to others for specific purposes, provided that purpose is deemed appropriate by the Clerk. Such a data user then agrees to delete the database from his possession after use. The Clerk keeps a record of such permissions and deletions.