

Hays Pension Trustee Limited (the "Trustee")

Data Protection Policy in relation to the Hays Pension Scheme (the "Scheme")

# 1. Introduction – responsibilities of the Trustee

1.1 In the course of managing the Scheme, the Trustee and its service providers collect and process information about members of the Scheme, and people linked in some way to members of the Scheme. The Trustee is legally responsible for ensuring that this information ("personal data") is processed in accordance with the law and with individuals' rights in respect of their personal data.

1.2 This policy sets out how the Trustee intends to comply with the key rules governing the use of such data, including the requirements of the General Data Protection Regulation ("GDPR"). For the purposes of this policy, "Data Protection Legislation" shall be taken to mean GDPR and any UK law concerning the protection of personal data, including any legislation which supplements or replaces GDPR. In deciding this policy, the Trustee has taken into account guidance available at the time from the Information Commissioner's Office (ICO) and the Article 29 Working Party.

1.3 The Trustee is a "data controller" for the purposes of GDPR.

1.4 GDPR does not apply to personal data of a deceased person. As a matter of practice, however, the Trustee intends to apply similar standards to its processing of data concerning a person who has died as it uses in relation to data about living persons.

1.5 This policy does not document every part of GDPR which may be relevant, but merely focuses on the key parts applicable to the Trustee. Should other issues arise in practice not covered by this policy, the Trustee will consider these separately at the time.

1.6 In this policy, and for ease of reference, the term "**Member**" will be used to refer to any individual in respect of whom the Trustee processes data (so including dependants, survivors and potential beneficiaries) except where the context requires otherwise.

1.7 The Trustee may amend this policy from time to time as it thinks fit.

# 2. Data protection principles

Under Data Protection Legislation, the Trustee is responsible for ensuring that personal data is processed in accordance with the data protection principles. In summary, these are that personal data:

(a) should be processed lawfully, fairly and in a transparent manner;

(b) should be collected for specific and legitimate purposes, and must be processed in accordance with those purposes;

(c) should be adequate, relevant and limited to what is actually necessary for the legitimate purpose for which it is collected;

(d) must be accurate and kept up to date;

(e) will be stored for no longer than is necessary; and

(f) must be processed in a manner which ensures appropriate security for personal data.

For the purposes of GDPR, "processing" includes collecting and storing personal data.

# 3. Lawfulness of processing and Conditions for Processing Special Category Data

3.1 **Lawfulness of processing**

(a) Under Article 6 GDPR, the Trustee may only process personal data where one or more lawful grounds apply.

(b) Having taken advice, the Trustee is satisfied that its processing of personal data relating to pension scheme members is lawful on one or more of the following grounds:

(i) The processing is necessary for the purposes of the legitimate interests (for the purposes of Article 6(1(f) GDPR) pursued by the Trustee in its capacity as trustee of the Scheme and by the Scheme's participating employers to help them make decisions relevant to their role in respect of the Scheme. The Trustee has legal duties to administer the Scheme in accordance with the trust deed and rules and with applicable pension law and it is in members' interests that it should do so. Administering the Scheme; paying benefits as required under the trust deed and rules; and making decisions relevant to the Scheme would not be possible without the processing of personal data. Members clearly benefit from having the Scheme properly administered and benefits paid when due. Accordingly, the Trustee considers that the fundamental rights and freedoms of the Members do not override the Trustee's and participating employers' legitimate interests in processing their personal data.

(ii) The processing is necessary for compliance with a legal obligation to which the Trustee is subject (see Article 6(1)(c) GDPR). The Trustee has legal obligations to the Members under the trust deed and rules and general law. In addition, pension scheme trustees are subject to general obligations relating to the operation of their occupational pension scheme. As an example, section 249A of the Pensions Act 2004 requires occupational pension scheme trustees to establish and operate internal controls, which includes maintaining accurate, up to date and secure records.

3.2 **Special category data**

(a) GDPR classifies certain categories of personal data as special category data. The Trustee is most likely to process special category data in respect of a Member in relation to considering eligibility for ill health benefits, or benefits payable on death.

(b) Under Articles 6 and 9 GDPR, the Trustee may only process special categories of personal data where:

(i) a lawful basis under Article 6 applies; and

(ii) the processing satisfies a condition under Article 9.

(c) The Trustee considers that its processing of special category data is necessary for the purposes of its legitimate interests, for the reasons set out in section 3.1(b)(i) of this Policy.

(d) The Trustee has been advised that its processing of special category data is necessary for the purposes of carrying out its obligations and giving effect to specific rights of Members in the field of employment, social security and social protection law, as expected to be authorised by the Data Protection Bill. Therefore its processing is expected to fall within the condition in Article ~~9~~9.2(b) GDPR.

(e) Accordingly, the lawfulness of the Trustee's processing of special category data is usually not expected to be based on consent. However, there may be circumstances in which the Trustee decides to base their processing of particular special category data on the Member's explicit consent, including if the relevant provisions of the Data Protection Bill are amended before the Bill receives Royal Assent. The Trustee understands that when processing is based on consent the Member will have additional rights in relation to his or her personal data.

# 4. Record keeping

The Trustee is required to maintain a record of its processing activities, containing specified information (see Article 30 GDPR). To enable the Trustee to comply with this requirement it will:

(a) analyse which entities process data on behalf of the Trustee ("Data Processors");

(b) ask each Data Processor to complete a Record of Processing Questionnaire (the "Questionnaire") which asks it to detail (among other things): what data the Data Processor holds on behalf of the Trustee; the categories of processing carried out for the Trustee; what procedures are in place to test and maintain accuracy of the data; and whether the Trustee's data is (or may be) transferred to a third party processor or transferred outside the European Economic Area;

(c) review the categories of processing carried out by the Data Processors to ensure that each processing activity falls within one or more lawful grounds for processing (please see section 3 of this policy);

(d) collate the responses to the Questionnaires and the lawful grounds for processing and keep a record of the collated information;

(e) carry out and record the results of a similar analysis in relation to any data processing carried out by the Trustee itself; and

(f) require each Data Provider to confirm annually whether or not there have been any material changes to the information provided in its Questionnaire.

4.2 To ensure compliance with the principles at 2(c) above, the Trustee will review each of the Questionnaires to satisfy itself that each Data Processor actually needs the data that it is processing and, where the Trustee thinks this is not the case, discuss the appropriate next steps with the applicable Data Processor.

4.3 The process of collating and reviewing the Questionnaires may inform any negotiations the Trustee has with its Data Processors about their ability to sub-contract services.

# 5. Retention of data

5.1 The Trustee recognises that Members' personal data should not be held longer than is necessary, and that in some other industries destroying data after a set period (for example, six years) may be common practice. However, the Trustee considers that it is important to retain Members' personal data for a much longer period of time. In reaching this conclusion, factors the Trustee has taken into account include the following.

(a) Obligations under the Scheme are inherently long-term: the Trustee could be paying a pension (or survivors' pension) to or in respect of someone who first became a member of the Scheme 80 years earlier.

(b) There are numerous examples of disputes about what a member's benefits under a pension scheme should be, or whether an individual is a member of a scheme. Resolution of such disputes often involves consulting documents that date back over several decades.

(c) Issues surrounding the reconciliation of guaranteed minimum pensions (GMPs), which members first started to accrue from 6 April 1978, are a further example of the importance of the long term retention of data.

(d) Long term retention of data is commonly considered appropriate and proper by those in the pension industry responsible for running pension schemes similar to the Scheme.

(e) Insurers may require retention of data in order for any claims to be investigated and their validity assessed.

5.2 Following consideration of the factors above,

 the Trustee has decided to retain data, and documents which contain data (together the "Records") indefinitely, in accordance with the policy set out in Schedule 1.

**6.** PRIVACY NOTICES

6.1 **General provisions about privacy notices**

(a) Subject to paragraph 6.5 below, the Trustee will ensure that all Members have access to a notice (a "Privacy Notice") containing information about how their data will be used. The Privacy Notice may be: sent directly to individuals; made available on a website; or provided on request to Members without access to the internet

(b) The Privacy Notice will include:

(i) the Trustee's details (as the data controller);

(ii) details of the purposes for which the Trustee processes personal data and the legal basis for that processing (as set out in section 3 above);

(iii) the likely recipients of personal data. The Trustee will explain this by reference to a non-exclusive list of the types of processor (for example, the scheme actuary or administrator) rather than by specifically naming individuals or firms;

(iv) the time the Trustee intends to hold the data (see section 5 above); and

(v) any supplementary information required by Article 13 GDPR or by other applicable data protection legislation.

(c) To ensure compliance with Data Protection Legislation, the Trustee will issue the Privacy Notice to all deferred and pensioner members (and beneficiaries in receipt of a benefit) in advance of GDPR coming into force in May 2018. After this is done, the Trustee will issue the Privacy Notice (or notification of how to access the Privacy Notice) to:

(i) applicants for ill health benefits;

(ii) new recipients of survivors' benefits;

(iii) members providing updated personal information.

(d) The Trustee will review the Privacy Notice annually and will amend it to reflect any changes in Data Protection Legislation or in the Trustee's practice.

## 6.2 Data about potential survivors

(a) Members may provide information about other individuals (such as their partner or children) who would, or might, become entitled to a benefit from the Scheme on the member's death. The Trustee has taken advice and has concluded that it may legitimately retain such information for the purposes of properly administering the Scheme. Any such information is held for the purposes of valuing the Scheme’s liabilities and paying benefits should the member die. This information is held either on the member’s record or in a sealed envelope in a locked filing cabinet in a separate room, entry of which is by security code.

 (b) After a member's death, the Trustee may receive information about potential recipients of a death benefit from third parties, such as solicitors or other family members. Such information is usually given subject to a duty of confidentiality. Its processing is necessary to enable the Trustee to identify to whom a benefit should be paid and, where the Trustee must exercise its discretion, so that the Trustee can comply with its duty under trust law to take into account all relevant factors.

(c) The Trustee has taken advice and notes that a Privacy Notice under Article 14 GDPR need not be provided where:

(i) provision of the information would prove impossible or would involve a disproportionate effort or where providing the information would render impossible or seriously impair the achievement of the objective of the processing; or

(ii) the personal data must remain confidential subject to an obligation of professional secrecy.

(d) The Trustee, having taken advice, considers that it would not be appropriate – by trying to send a quasi-privacy notice to someone – to disclose to that person that the Member had nominated them for a potential death benefit. That information should be kept confidential. The Trustee also considers it would not be appropriate to send a Privacy Notice to individuals where personal data has been disclosed by a solicitor or provided by a third party;

(e) The Trustee will keep this approach under review – including taking into account any guidance produced by ICO, industry standards set by appropriate bodies, the requirements of trust and pension law, and practice among trustees of similar pension schemes.

# 7. Rights of Members

## 7.1 Data subject access requests

(a) Members are entitled to access their personal data held by the Trustee on request (Article 15 GDPR). The response to a data subject access request must also include certain other 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. To assist compliance with GDPR, the Trustee has adopted the standard data subject access response attached to Schedule 4 of this policy and has required its administrator to assist the Trustee in responding to legitimate data subject access requests.

(b) The Trustee has noted that, under GDPR, the information must be provided to Members free of charge and within one month of the request.

## 7.2 Right to be forgotten

(a) Members have the right to require the Trustee to erase all data held in respect of them in various circumstances (Article 17 GDPR). The circumstances include if the individual withdraws consent to processing the data and there is no other legitimate ground to justify the processing (see section 3 above). However, the Trustee need not delete the data if an exception applies, including that the processing is necessary to comply with a legal obligation.

(b) The Trustee considers it unlikely that any member will seek to exercise this right and has decided to review any request, and take advice, should the situation arise. However, to prepare to meet the requirement, the Trustee has decided to prepare standard letters to be used in response to such a request attached to Schedule 4.

## 7.3 Right to rectification

(a) Members have the right to have incorrect personal data about them corrected without undue delay (Article 16 GDPR). The Trustee endeavours to have its data as up to date and correct as possible and to comply with the expectations of the Pensions Regulator. Where an error is discovered, the Trustee (or its administrator) already corrects this as soon as possible.

(b) The Trustee therefore considers it unlikely that any change of practice is needed but will take advice as necessary if it ever receives a formal rectification request. To prepare to meet the requirement, the Trustee has decided to prepare standard letters to be used in response to a request attached to Schedule 4.

## 7.4 Right to data portability

(a) Members 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 Trustee to another data controller (Article 20 GDPR). The Trustee has been advised that the circumstances in which the right to data portability arises are limited and, at present, seem unlikely to apply to most pension scheme members.

(b) The Trustee has decided to take no action in relation to data portability at the current time but will monitor the situation and take advice should this become necessary in future.

# 8. Data security

## 8.1 Data security on the part of the Trustee Directors

The directors of the Trustee (the "Trustee Directors") have responsibility to ensure that in performing their duties they do not endanger the security of personal data. The Trustee Directors have accordingly adopted the policy (the "Trustee Director Personal Security Policy") included in Schedule 2 to this policy. The Trustee Directors may review, amend and update the Trustee Director Personal Security Policy from time to time.

# 9. Use of Data Processors

9.1 The Trustee shall ensure that it has a written contract which meets the requirements of GDPR in place with each Data Processor. In particular, the Trustee will expect each Data Processor to guarantee that it will meet the requirements of GDPR and will protect Members' rights.

9.2 Before engaging a new Data Processor, the Trustee will check that:

(a) the Data Processor has appropriate technical and organisational measures in place to keep data secure; and

(b) the Data Processor's staff who will be engaged in processing data in relation to the Scheme are subject to a duty of confidentiality and receive regular training in data protection matters.

9.3 The Trustee will seek appropriate assurances from each Data Processor as to the security arrangements it has in place. This may take the form of:

(a) for an existing Data Processor: a short summary of its key data security measures;

(b) for a new Data Processor: before entering into a new contract, a short statement of its key data security measures; and

(c) subsequent confirmation from each Data *Processor every* 24 months of what, if any, changes there have been to its security arrangements.

9.4 The Trustee recognises that its Data Processors may wish to sub-contract some services, which may include sub-contractors processing data on behalf of the Data Processor. The Trustee will ensure that its contract with each Data Processor contains provisions concerning sub-contracting which meet the requirements of GDPR.

# 10. Data security breaches

10.1 The Trustee takes seriously the need to deal with any data breach swiftly and appropriately to minimise or eliminate risk of detrimental impact on any Members. For this purpose, a data breach may include (but is not limited to): unauthorised disclosure of or access to personal data; or accidental or unlawful destruction of personal data; or loss or alteration of personal data.

10.2 The Trustee shall require its Trustee Directors, its own staff (where applicable) and its Data Processors to report data breaches to Kath Bedford, the Pensions Manager, or, if unavailable, Doug Evans, Hays Company Secretary and Trustee promptly and to assist the Trustee in ensuring compliance with the requirements of GDPR.

10.3 On being notified of a data breach, Kath Bedford will as soon possible notify each Trustee Director.

10.4 Where a data breach has occurred, the Trustee and Kath Bedford shall consider whether it is necessary or appropriate to notify the Information Commissioner's Office ("ICO") or affected Members of the data breach, and will take professional advice as a matter of urgency where required.

10.5 The Trustee will maintain a record of any data breaches and action taken in relation to each breach in the form set out in Schedule 3.

# 11. Data Protection Officer and Data Protection Impact Assessments

11.1 The Trustee has taken advice on the requirements under Data Protection Legislation to appoint a data protection officer ("DPO") or to carry out a data protection impact assessment ("DPIA") in certain circumstances.

11.2 The Trustee has been advised that it is not currently required to appoint a DPO because it does not fall within the remit of Article 37(1) of GDPR for the following reasons;

(a) the Trustee is not a public authority or body;

(b) the core activities of the Trustee do not consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systemic monitoring of data subjects on a large scale;

(c) the core activities of the Trustee do not consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

11.3 An organisation 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.*"

11.4 The Trustee does not believe that the nature of its processing (which - as set out in section 3 above - is fundamentally to ensure the correct benefits are paid to the correct Members) is such that there is likely to be a high risk to the rights and freedoms of Members and it has concluded that it is not necessary for it to undertake any DPIAs.

11.5 The Trustee will keep the position on whether it needs to appoint a DPO or carry out a DPIA under review, taking into account any guidance issued from the ICO.

Adopted by the Trustee:

Signed: ……………………………………….

Adopted on: ………………………………….

Schedule 1

Record retention policy

The Trustee has decided to retain data and documents which contain data (together the "Records") indefinitely but subject to review on the earlier of the Scheme winding up or changes to the GDPR.

The Trustee will not therefore automatically review its retention of data policy annually for the reasons detailed in section 5.

Schedule 2

Trustee Director Personal Security Policy

1. Trustee Directors will ensure that personal data is kept secure and protected from unauthorised or accidental access, loss or disclosure to parties who do not have a right to access it. Recognising that many of the Trustee Directors do not have business email addresses, and so access information from personal computers, this will be achieved by:

1.1 The Trustee Directors being required to use a secure internet site to access documents which contain personal data. Hays plc will make available an email address for Trustee Directors who are not current employees, if required; and

1.2 that internet site being designed that the Trustee Directors can make decisions in relation to personal data (for example decide about the payment of discretionary benefits) without needing to print-off documents or save them to their personal computer hard-drives.

2. Trustee Meeting papers are accessed via a secure site, Diligent. Any hard-copy meeting packs sent to Trustee Directors will be in sealed packaging marked "addressee only" and sent by recorded or registered delivery.

3. Where Trustee Directors use a shared PC or other device to access the secure internet site, they shall ensure that the PC or device is not left unattended when logged on to the secure internet site.

4. Access to personal data shall be restricted to Trustee Directors or their professional advisers or administrators who require such access to carry out their duties. Professional advisers, who have business email addresses, may either access the same data-site, or may receive emails to their business email address attaching documents containing personal data that are always password protected. Trustee Directors or their professional advisers or administrators who receive emails or personal data on portable storage media (such as laptops and USB drives), must ensure that they are encrypted, using industry standard encryption techniques, to reduce the risk that the security of personal data might be compromised in the event the storage device is lost.

5. When a Trustee Director resigns from his/her role, they shall, at the direction of the Trustee, promptly delete or return any personal data they are holding in respect of the Scheme members.

Schedule 3

Record of data breaches

|  |  |  |
| --- | --- | --- |
| Date of breach | Explanation of breach and what it related to | Action – including whether notification was made (and the reasons why/why not) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Schedule 4

Record of agreed Letters to members /dependants / beneficiaries

To assist compliance with GDPR, the Trustee has adopted a number of letters covering the following rights of members.

1. Data subject access requests
2. Right to be forgotten
3. Right to rectification