The Association of Directors of Public Health

Data Protection Policy

1. Introduction

1.1. The Association of Directors of Public Health (also referred to as ADPH, the Association) is the professional membership association for statutory directors of public health working in local authorities in the UK. These members are referred to as Ordinary Members. The ADPH also has Associate members, who are current Consultants in Public Health who work for a Full Member of ADPH, persons who perform like functions to a Consultant in Public Health and whose functions in the opinion of the ADPH Board equate to the role of a Consultant in Public Health, and persons in nationally defined Public Health roles that, in the opinion of the ADPH Board, merit Associate membership status. The Association also offers former Ordinary Members who are no longer in the employment of a local authority public health department the opportunity to apply for Alumni Membership.

1.2. The Association is a Private Company Limited by Guarantee and Registered Charity in England and Wales.

1.3. The ADPH processes information about each individual member. Ordinary and Associate members register with the Association using their professional information contact details and Alumni using personal contact details.

1.4. The Association has taken all necessary steps to ensure compliance with the General Data Protection Regulation (GDPR) and is registered with the UK Data Protection Authority, the Information Commissioner's Office (The ICO).

2. Reasons/purposes for processing information

2.1. The Association processes information about each member to administer membership records; to communicate with members on issues pertinent to the work of the association; and, to administer the involvement of members with, and on behalf of, the association.

2.2. It is important that the personal data held by the Association is accurate and current and it requests therefore that it is kept up to date on changes during membership.

3. Data Protection

3.1. The Association will adhere to the key principles of data protection:

- Process data fairly, lawfully and with transparency
- Follow the Purpose Limitation Principle – data collected for one purpose will not then be used for another purpose
- Data minimisation – data will be processed as necessary. Steps will be taken to erase or cleanse data unnecessary data. ADPH will not collect data in case it is useful in the future
- Accuracy – ADPH will endeavour to maintain accurate records across all systems
- Data retention – ADPH will not hold data longer than necessary
- Data security – ADPH will ensure electronic and physical data is secure, including that processed by any 3rd parties
- Accountability – at all times ADPH will endeavour to take all reasonable steps to ensure the association is compliant with data protection laws.

4. Consent

4.1. ADPH will only process members' data when given explicit consent to do so by each individual member. Consent will be obtained in an appropriate and distinguishable manner.

4.2. ADPH will explain clearly, intelligibly and precisely the scope, purpose and context of data processing.

4.3. All ADPH members have the right to:

- Request access to your personal data (commonly known as a "subject access request"). This enables members to receive a copy of the personal data held and to check that it is being lawfully processed.
- Request correction of the personal data held by the Association. This enables members to correct any incomplete or inaccurate data. ADPH may need to verify the accuracy of the new data provided.
- Request erasure of personal data. This enables members to ask us to delete or remove personal data where there is no good reason for us continuing to process it. Members also have the right to ask us to delete or remove personal data where they have successfully exercised their right to object to processing (see below), where the Association may have processed information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that the Association may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- Object to the holding and processing of personal data if it is felt to be incorrect.
- Request restriction of processing of personal data. Members can request the suspension of the processing of personal data if they want us to establish the data's accuracy or where use of the data is unlawful but do not wish it to be erased.
- Request the transfer of personal data to themselves or to a third party.
- Withdraw consent to hold data at any time. This will not affect the lawfulness of any processing carried out before withdrawal of consent. If consent is withdrawn ADPH may not be able to provide certain products or services to members and will advise if this is the case at the time you withdraw your consent.

4.4. ADPH members can exercise all rights by contacting the association by telephone or in writing by email or letter.

4.5. ADPH will ensure all data provided will be portable and easy to access if requested.

4.6. ADPH members have the right at any time to make a complaint concerning data protection issues to the ICO.

5. Access rights cover

5.1. All rights (see 4.3) can be exercised free of charge and within one month. However, a reasonable fee may be charged if requests are repetitive, unfounded or excessive.

5.2. ADPH will delete all personal data:

- If data is no longer needed for the purpose it was collected for
- If consent is withdrawn
- If an objection is submitted.

5.3. ADPH will restrict processing if:

- Accuracy is contested
- Processing is suggested to be unlawful
- Data is required for legal cases
- Pending request for erasure.

6. Data controller

6.1. The data controller, by definition, is the organisation; therefore, the Association is the data controller. ADPH has assigned the role of data protection officer (DPO) to a member of the staff team, Mark Hamblett.

6.2. The controller is accountable for:

- Implementation of technical measures
- Privacy policies
- Staff training
- Monitoring adherence and conduct rules
- Evidence compliance.

6.3. The DPO will ensure records are kept of processing activities and ensure that data processing information is available to the relevant data protection agency (The ICO).

7. Security

7.1. IT systems:

7.1.1. ADPH maintains robust IT systems. Individual workstations are secured using Microsoft antivirus and spyware. All servers and workstations are password protected.

7.1.2. Data processing is carried out following set procedures.

7.1.3. ADPH runs both cloud based and physical back-up of all data.

7.1.4. All ADPH cloud based applications store data in Microsoft datacentres based in the UK and Salesforce datacentres based in the EU. ADPH does not store data outside of the EEA but remains mindful of cross-border data transfer agreements/EU-US Privacy Shield regulations when dealing with 3rd parties.

7.2. Financial records

7.2.1. ADPH operates in line with legal regulations and securely retains financial records for the appropriate duration.

7.3. Secure document disposal

7.3.1. ADPH ensures that all physical records containing personal data are securely destroyed if no longer needed.

7.4. Data breaches

7.4.1. Should a data breach occur ADPH will notify the data subject as soon as possible and no longer than 72 hours from its discovery.

7.4.2. ADPH will notify the ICO of a data breach within 72 hours. Detailed records of the breach and process to deal with the breach will be kept.

8. Third party processors

8.1. ADPH occasionally employs, or has agreements with, third party organisations or individuals to carry out business functions on behalf of the association or in relation to providing membership services.

8.2. ADPH ensures that written binding agreements are in place with these processors.

8.3. Processors are only able to act to instruction and must treat all data with confidentiality. Data must be secure and all data should be returned or destroyed following the purpose of the third-party contract.

8.4. Third party processors must be able to demonstrate that they are GDPR compliant.

9. Contact

9.1. The ADPH Data Protection Officer is Mark Hamblett.

9.2. All enquiries in relation to data protection and this privacy policy should be directed to the Data Protection Officer.

9.3. Contact details are as follows:

- The Association of Directors of Public Health, Fleetbank House, 2-6 Salisbury Square, London EC4Y 8JX
- Email: enquiries@adph.org.uk or mark.hamblett@adph.org.uk
- Telephone: 020 7832 6946
- Registered in England and Wales. Company Number: 8448934. Registered Charity Number 1164513.