The Association of Chief Executives Privacy and General Data Protection Regulations Policy

Introduction

Data protection legislation sets out the responsibilities of organisations that use and store personal data. The purpose of this policy is to inform members and non-members how the Association of Chief Executives, (hereafter referred to as ACE or the Association), will store and use personal data and information about its membership.

The General Data Protection Regulations 2016 (GDPR) come into force on 25 May 2018. They apply to ACE, as a controller and processor of personal data, requiring the organisation to take steps to ensure it is using personal data lawfully. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. The contact details for the data controller are stated at the end of this document.

What kind of personal data ACE holds

Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Work and personal email addresses constitute personal data under GDPR. This is the personal data held by ACE. ACE does not hold any other form of personal data or sensitive personal data, as defined by GDPR. Members of ACE are the chief executives and their direct reports of public bodies, and consequently their names and positions are in the public domain. However, neither their, nor their support staff, email addresses are always publically available. ACE also holds the personal data, i.e. email addresses of stakeholders, such as civil servants in government departments, and the National Audit Office.

How personal information is collected

ACE obtains personal data in a number of ways. On joining the Association, members provide contact details so that the Association can keep them informed about relevant matters. Personal data may also be collected from central government, (including directly from departments or publications such as Public Bodies 17). Data may also obtained from the public body, either through their website or by contacting personnel in the organisation.

How we will use personal data

ACE shall ensure that the personal data it holds is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

ACE will implement this policy in the following way:

The intended purpose for processing personal data, the use of individual's email addresses, is a necessary part of the Association's contract with members in order to ensure members are provided with information relevant to their membership. Such purposes include:

- contacting members for matters relating to their organisation's subscription, including for financial queries;
- providing member updates; newsletters; event information; and
- research it is involved in.

ACE considers that its members would reasonably expect the organisation to use its personal data in this way, having joined the organisation with an expectation of receiving this information, and that it would have minimal privacy impact. ACE considers using the personal data in this way to be its legitimate interest. A copy of our Legitimate Interest Assessment is contained at Annex 1 of this policy.

ACE will provide the option for members to 'opt out' at the end of its emails. Members can withdraw consent by emailing secretariat@associationofchiefexecutives.org.uk and the organisation will act on the withdrawal of consent at swiftly as practicable. ACE will maintain a record of the consent provided.

ACE may contact non-members, using the email address of a public body, in order to maintain its business model more generally. This includes approaching the Chair of an organisation asking them to become a member; inviting them to an event; contacting them in relation to a piece of research ACE is conducting; and asking whether they consent to being contacted by a third party with whom ACE has a partnership. ACE considers that the Chair may reasonably expect the organisation to use its personal data in this way, and that it would have minimal privacy impact. Advice received from the Information Commissioner's

Office supports this approach. ACE considers using the personal data in this way to be its legitimate interest. ACE will not use the personal email addresses of non-members in this way, unless the individual has provided consent to being contacted. For the purposes of openness and transparency, at the end of emails sent by members of the ACE Secretariat, the signature will contain information on how to 'opt out' of future email correspondence. The organisation will act on the withdrawal of consent at swiftly as practicable.

ACE will maintain a 'suppression list' of people who have opted out or otherwise told ACE directly that they do not want to receive marketing. This will ensure the person's preferences are respected in the future, and not contacted in error. The list will only contain their name and the name of the public body they are associated with. ACE will not contact people on a suppression list at a later date to ask them if they want to opt back in to receiving direct marketing because this would breach the Privacy and Economic Communications Regulations. In the event that the Chair of the public body changes, ACE may contact the new Chair.

Reducing the amount of personal data held

ACE is committed to amending and deleting personal data it holds at the request of an individual, unless it is required to do so to fulfil a legal obligation. ACE does not undertake any automated decision-making, where a decision is made solely by automated means without any human involvement.

The ACE will minimise the amount of personal data held by undertaking the following processes by the 31 July 2018.

- ACE will conduct an audit to assess information held on our systems, including systems provided by external providers such as Survey Monkey and Xero, and delete personal data that does not fall within the scope of the policy. ACE holds personal data on the invoicing system Xero.

- It will delete the email addresses of past members but retain the record of transactions for financial auditing purposes.

- ACE will retain historic lists of organisations that have been members but will delete the personal data of past members by 31st July 2018.

Work with third parties

The ACE and the Public Chairs' Forum, (PCF), share a secretariat and therefore the personal data of each organisation's members is available to the other organisation. The organisations work together on occasion to host joint events and pieces of research that their boards consider beneficial to both sets of members. Therefore, members' data may be shared with the PCF.

ACE frequently works with third parties, including the Institute for Government, (IfG), Cabinet Office, and Whitehall and Industry Group. ACE will not share the personal data of its members with third parties, including the IfG, government officials, other members, or private organisations. In the event that the IfG, Cabinet Office, another organisation, or a member wishes to make contact with ACE members, the ACE secretariat will either contact the specific member on their behalf to ask whether they consent for their personal data to be passed on, or, in the event that the third party wishes to pass on information to a number of

members, and the information is relevant to their role as the leader of a public body, the ACE Secretariat will forward the information on their behalf.

ACE may disclose to central government departments, the IfG and the Whitehall and Industry Group the names of the organisations that are members but not the personal data that it holds. The names of those who lead the organisations that are members of ACE are a matter of public record.

Subject access requests

In the event that a person makes a subject access request, ACE will not normally charge for this. ACE will aim to comply with the request within one month and where this is not possible, inform the person of any delays. ACE will only refuse a subject access request, or charge for complying, if the request is considered manifestly unfounded or excessive. The decision to refuse a subject access request or to charge for it will be made by the ACE Board. In this event, the person making the request will be informed of the reason why it has been refused and of their rights to complain to the Information Commissioner's Office, within a month of the Board making the decision.

Data breaches

In the event that ACE discloses personal data without the consent of the person to whom it belongs, the Secretariat will take the following steps within 24 hours of becoming aware of the breach:

- Inform the individual that their personal data has been disclosed, to whom, and when.
- Inform the Information Commissioner's Office, (ICO), and the chair and board of ACE, including the circumstances of the breach.
- Inform the person to whom the data has been disclosed what has happened, request that they delete the information, and provide written confirmation that this has been done. The written confirmation will be provided to the person to whom the data belongs. It will also be provided to the ICO if requested. ACE will instigate an investigation to establish how the data breach happened and report the findings of the investigation to the person to whom the data belongs, the Board and the ICO.
- The secretariat will maintain a record of all data breaches, which will be made available to its members, the Information Commissioner's Office and government departments on request.

Information technology used by ACE

The ACE Secretariat is based at the IfG, which provides IT and supporting technology. The system belongs to the Institute. Under the terms of the agreement with Institute, it will make use of technology including firewalls, anti-virus, anti-malware and SSL encryption, which aims to:

- Ensure the confidentiality and protection of information against unauthorised access

- Maintain the integrity of all information and ensure the availability of all information as required
- Maintain disaster recovery and business continuity plans for its business activities
- Ensure that breaches of Information Security, actual or suspected will be reported/investigated

The systems and technology described above are used by ACE.

Other matters

The ACE does not hold any special category data or personal data about children and therefore does not need to make special provisions relating to such data.

In the event that consideration is given to share data in a new way, or design technology that uses personal data, a Data Protection Impact Assessment will be undertaken.

The ACE only operates within the UK and does not transfer any data outside of the European Economic Area.

Contacts

This policy has been signed off the ACE's Board. The Manager of the Secretariat will take responsibility for data protection compliance. They will ensure all data protection matters are reported to the Board in a timely fashion, if necessary outside of a scheduled meeting. All those working within the Secretariat are required to comply with the policy. To contact the manager, please email secretariat@associationofchiefexecutives.org.uk.

Should a person wish to complain about the way ACE controls or processes personal data, they should contact the Information Commissioner's Office in the following way:

- By telephone: 0303 123 1113
- Via the ICO website: https://ico.org.uk/concerns/

Annex 1

Public Chair's Forum GDPR Legitimate Interest Assessment

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

The Association of Chief Executives wants to process individuals' personal data for the following reasons:

- Inform our members about events and research being undertaken by ACE
- Send invoices relating to their membership
- Conduct pieces of research
- Invite them to join ACE
- Communicate with stakeholders, including government departments, the Institute for Government, the National Audit Office, about the work being undertaken.

The ACE will benefit from processing the data for the following reasons:

- members will receive information relevant to their membership, in turn this will maintain membership levels.
- The Association will be kept updated with relevant information from its stakeholders, which can be used to determine the work of the Association.

Third parties may benefit from the processing because membership of the Association can have a positive impact on the organisation and the wider public body community.

The benefits identified are important for our members because they are more likely to receive value for money of their membership if they are aware of the Association's events and research.

The following negative impacts could be felt if the data was not processed:

- Members would not be aware of the events they are entitled to attend as part of membership or of research being undertaken that they could be involved in or benefit from the outcome.
- The Association may lose members.
- The Association is less likely to be aware of matters elsewhere that its membership would be interested in.

ACE considers that use of the personal data in the manner set out complies with e-privacy legislation for the following reasons:

- Emails inviting organisations to join ACE would be sent to corporate bodies – non-work personal emails addresses would not be used for this purpose.
- Communications from ACE will contain the option to 'opt out' of future communications. ACE will maintain a list of these organisations.
- Communications from the ACE will be clear and provide a valid contact address so they can opt out of future emails.
- Direct marketing rules do not apply when organisations such a ACE are conducting research.

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

ACE exists to improve the efficiency and effectiveness of the delivery of public services. It does this by providing information sharing and networking opportunities for the chief executives and their direct reports of public bodies at a programme of tailored events. By drawing on the perspectives of its members, the ACE is able to provide information, advice and guidance to Government on the role of arm's-length bodies in the delivery and reform of public services. If members did not attend the events, then it would be difficult for the Association to achieve its purpose.

ACE considers the use of the personal data as set out above to be proportionate to our purpose. It would not be possible to achieve our purpose without processing personal data.

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data

The ACE does not control or process any special category data or criminal offence data. Neither does it hold any data that people are likely to consider particularly private. The ACE does not control or process any data relating to children or other vulnerable people.

From time to time, ACE members provide the Association with a personal email address that is not connected to their public body. They are usually provided so that the Association can keep them updated with matters related to their membership. Personal email addresses of past members will not be retained.

The data held will relate to people's professional capacity.

Reasonable expectations

ACE has existing relationship with those it is in contact with either because they have contacted the organisation to become a member, or in relation to our work with central government.

The nature of the relationship is professional. We contact members to provide them with information relevant to their membership, and to keep stakeholders that are not members informed about matters they may find relevant to their work.

We do not provide their data to third parties. In the event that a third party wishes to contact them, then we ask whether they are content to be approached by them.

Data from members is either provided by them directly or the organisation they work for, or from publically available documents, such as Public Bodies 17.

Data for stakeholders is provided by the organisations they work for.

Members are informed that they will be added to our mailing list. They will be provided with a copy of our Privacy and GDPR policy. This sets out how we intend to use data.

Membership data has been collected over the past ten years. Obsolete data about past members will be deleted.

Likely impact
Members will not see a change in the way that their personal data is being used by ACE. ACE does not consider that the impact on processing people's personal data will be negative because members expect to receive updates about our work, and we regularly keep in touch with our stakeholders, including providing them with copies of our newsletter. Individuals will not lose control over their personal data. The ACE considers that the impact of processing the data is minimal. ACE does not believe people will find use of their personal data in the way we have set out to be intrusive. A copy of the privacy policy will be provided. Members and stakeholders can elect to opt out from their data being processed by ACE.

Can you offer individuals an opt-out?	Yes

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes
Do you have any comments to justify your answer? ACE believes our members expect to be provided with information relevant to their membership. Other stakeholders are contacted in relation to matters relevant to their work and that of ACE. ACE does not use personal data for marketing and the privacy policy provides clarity on how we work with third parties.	
LIA completed by	Emma Maloney, Manager
Date	18 May 2018