CAPALC
PO Box 181
St Ives
PE27 9DR
Tel: 01480 375629
www.capalc.org.uk

Cambridgeshire & Peterborough Association of Local Councils

CAPALC General Data Protection Regulations Membership Scheme

Details of service agreement between Priviness Ltd (the provider)
and
Cambridgeshire and Peterborough Association of Local Councils and its Members (the customer)

The Details of Service
The aim of our service is to provide the expertise, guidance and tools to manage your GDPR programme. To meet your GDPR obligations, our optional services we provide you may include:

1. On-going support provided via our consultancy and customer service resources for CAPALC and its members, including pre-populated templates, guidance, awareness training and policies to develop a suitable and coherent GDPR strategy, covering such aspects as:

    - purposes
    - legal bases
    - safeguards
    - risk assessments
    - privacy information notices
    - rights workflow
    - personal data breach procedures
    - internal guidance for social media, CCTV, etc
    - incident management guidance
    - disaster recovery and business continuity templates

    We will guide and assist you in the completion of these documents, providing an agreed number of hours per month retained support within a pre-agreed cost structure, where additional support will also be available at an additional cost where and as appropriate

2. Readiness review – this is a moment in time analysis of current compliance against GDPR, and is delivered as a written document recording strengths and weaknesses, and recommended actions to further progress towards GDPR compliance.

3. Education for all staff and councillors, via access to an online video on GDPR.

4. Acting as a representative and data protection officer for CAPALC and its members

5. Access to other services (charged separately): for example, enhanced training, and other ad hoc advisory services including drafting codes of conduct.

"Our Services" are detailed on our website: http://priviness.eu/

Privacy and Confidentiality Services – your responsibilities

You (CAPALC and its Members) are legally responsible for:

- Ensuring that processing of personal data is lawful
- Ensuring that your DPIAs are completed
- Filing any submissions to the ICO
- Settling any fines from the ICO

Failure to do so may lead to automatic penalties, surcharges and / or interest.

Organisations cannot delegate their legal responsibility to others. You agree to check that reports that we prepare for you are complete before you approve and sign them.

To enable us to carry out our work, you agree:

1) That all submissions are to be made on the basis of full disclosure of all relevant information pertaining but not limited to:
   i) personal data, including sensitive categories,
   ii) specific purposes and timeframes that personal data is required,
   iii) the limit of personal data that is required for each purpose,
   iv) the end-to-end processes pertaining to personal data,
   v) any known legal basis for processing of personal data,
   vi) recipient organisations or data subjects of personal data, and
   vii) the locations of where personal data will be held, processed, accessed, or viewed.

2) To provide full information necessary for dealing with your privacy and confidentiality matters – we will rely on the information and documents being true, correct and complete.

3) To authorise us to approach such third parties as may be appropriate for information that we consider necessary to deal with your information governance matters; and

4) To provide us with the information in sufficient time in order that remedial measures can be undertaken in time to comply with GDPR.

As your GDPR representative or Data Protection Officer, you agree:

1) To keep us informed of material changes in your circumstances that could affect your risk pertaining to non-compliance with privacy and associated legislation. If you are unsure if the change is material or not please assume that it is, contact us, and we will assess the significance.

2) To forward to us ICO or other privacy regulator communications, legal challenges pertaining to privacy matters, and letters and other breach-related communications from data subjects in time in order to enable us to deal with them as may be necessary within the statutory time limits.

Charges and expenses

Our charging rates are reviewed from time to time, usually in April of each year.

Limitation and exclusion of liability
In common with other professional advisors, priviness ltd's policy, on matters (other than statutory data protection officer services) in which we are instructed, is to exclude and / or limit our liability to clients in certain situations.

Please note that, in particular, it will be priviness ltd that provides the services to you and that priviness ltd's liability to you will be limited to £1m on each matter on which it is instructed, unless prohibited by law or otherwise agreed in respect of that specific matter. The limit in respect of our total aggregate liability will not apply to data protection officer services.

Publicity
From time to time priviness ltd likes to include details of clients in its publicity materials. Unless we hear from you to the contrary, we shall assume that you are happy in principle for priviness ltd to publicise your name as a client of priviness ltd. Please do let us know if you have any objection to this. Details of particular matters priviness ltd has handled for you will not be included without your prior consent.

Privacy
Your privacy is of utmost concern to us. In signing this letter, please note that you are agreeing that priviness as a controller (see contact details above) will process personal data belonging to you and other individuals within your organisation and immediate supply chain, for the purposes of:

- communicating with you and your organisation on information governance matters pertaining to privacy, data protection, and confidentiality issues;
- sending documentation associated with any agreed work;
- sharing with our extended priviness team, external legal and other advisors as well as public and competent authorities to follow up on queries or issues arising from any agreed work – NB we do transfer contact details to our Customer Services, who are based in South Africa which is outside the EEA, to manage relationships, the safeguard measures we take to protect your information being available on request; and
- processing any payments relating to any agreed work.

We will retain your personal data for 2 years following the latest exchange of information as a condition of our contract in case there are queries. It may be necessary to disclose your said information to our providers in our legitimate interest. You have the following qualified Rights, subject to certain conditions;

- access to, rectification and/or erasure of your personal information;
- object to and/or restrict processing of information, including not being
- subject to a decision based solely on automated processing, including profiling;
- portability – where you have provided us with your information in
- electronic form, you may ask us to port your information to yourself or
- another controller in a structured, commonly – used, machine – readable, and interoperable form;
- complain to either the Data Protection Authority or to seek judicial remedy.