

## General Data Protection Regulation (GDPR)

The new General Data Protection Regulation (GDPR) replaces the Data Protection Act on May 25<sup>th</sup>, 2018. GDPR will increase individuals' rights on personal data and will therefore significantly tighten up the rules on privacy and consent. Councils will also need to audit legacy data to identify where it is held, whether consent was granted correctly and will need to delete records where it wasn't or where new consent cannot be obtained. Councils will need to ensure privacy is designed into current and future processes and services. Therefore, GDPR will change the way councils use personal data in the delivery of services.

As part of the implementation of GDPR local councils will need to secure the provision of a Data Protection Officer (DPO). The latest guidance from the public sector policy team at the Information Commissioner's Office (ICO) is that it is unlikely that clerks and Responsible Finance Officers can be the Data Protection Officer (DPO). Therefore, many councils are not going to be able to appoint a DPO internally due to difficulty in identifying any individual with sufficient independence from data controlling, collection, and processing. A DPO can be an external or internal appointment and, inter alia, they must carry out internal audit work to test ongoing compliance with GDPR.

## Our Services

As the internal audit provider, several councils have discussed this issue with us, including requesting that we provide a quotation for these services, as we already have a thorough knowledge of the council systems, policies, internal controls and already report independently to full council. Therefore, we are offering this service to larger councils that are unable to identify an internal resource to carry out this function, or where it is not cost effective to carry out the function internally.

## What we will provide:

- We will support the completion of a data audit and data inventory before May 2018 to provide a data flowchart that details the nature, scope, purpose, timings and location of council's processing activities and associated risks, using the ICO recommended toolkit. The council will then need to implement the recommendations arising from the data audit. If the scope of the council services change, this data flowchart should be updated.
- We will carry out internal audits of compliance with the GDPR requirements as part of our planned internal audit work and report findings and recommendations to full council.
- We will provide best practice toolkits and provide guidance in completing Privacy Impact assessments when these are required. We will audit compliance with the recommendations from the Impact Assessment.
- We will be the first point of contact both for the ICO and for the notification of a data breach.
- We will share best practice with officers and the council to raise awareness of data protection law and current key issues. We will maintain expertise through Continuing Professional Development training.
- Where requested we will provide independent opinion on council decisions that have data protection implications

It should be noted that it is the council that is responsible for compliance with data protection law and not the DPO whose key role is to independently assess compliance on an ongoing basis.

<b>SCALE OF FEES (excluding VAT)</b>				
<b>£ Precept Bands</b>	<b>25000 – 99999</b>	<b>100000 - 199999</b>	<b>200000 - 399999</b>	<b>400000 +</b>
<b>Year One Fees</b>	<b>£600</b>	<b>£900</b>	<b>£1200</b>	<b>£1500</b>
<b>Year Two Fees</b>	<b>£400</b>	<b>£700</b>	<b>£1000</b>	<b>£1300</b>
<b>Year Three Onwards Fees</b>	<b>Annual increment to reflect CPI (consumer price inflation)</b>			

If you wish to discuss Data Protection Officer requirements, please contact John Henry by email at [john@jdhbs.co.uk](mailto:john@jdhbs.co.uk)