Information Governance Survey: What councils need to do now

Posted on March 20, 2017 by icocomms

By Anulka Clarke, ICO Head of Good Practice.

We're here to help local councils comply with the Data Protection Act and get ready for the new General Data Protection Regulation (GDPR) coming into force from May 2018.

The ICO's Good Practice department conducted a survey at the end of last year to find out more about information governance practices in local government. It received 173 responses. We already knew from our work with councils that there are some positive measures in place at local authorities but wanted to find out more about patterns of existing practices.

The overarching conclusion from our analysis of the survey results was that, although there is good practice out there, with GDPR coming in May 2018, many councils have work to do. Adhering to good practice measures under the Data Protection Act (DPA) will stand organisations in good stead for the new regulations.

The stand-out findings from our survey are highlighted in the infographic below.

A quarter of councils told us they don't have a data protection officer. Under the new GDPR, public authorities must have one.

More than 15% of councils do not have data protection training for employees processing personal data.

A third of councils don't do privacy impact assessments. Under GDPR they will be legally required in certain circumstances.

The links in this blog will direct councils to some of the key areas they need to consider in their GDPR preparations. And, as always, we will continue to be on hand with practical advice on how to improve.

Adopt a privacy by design approach

Our survey results found that although most councils carry out privacy impact assessments (PIAs), 34% of councils still do not. That will need to change. GDPR makes it a legal requirement for councils to conduct data protection impact

assessments in certain circumstances. Our Privacy Impact Assessment Code of Practice provides more advice and will be reissued for GDPR in due course.

Councils will benefit from producing their own PIA process and accompanying guidance to ensure privacy issues are considered as part of projects.

When it comes to other important policies, it was good to see that 93% of councils have a data protection and information security policy. But 37% of councils have no data sharing policy, despite increasing data sharing requirements to provide certain services. Our data sharing guidance can help change that.

Councils should make sure all their data protection policies are reviewed annually.

Have the right staff in place

A quarter of councils told us they don't have a data protection officer. Under GDPR the role of data protection officer is required in public authorities.

It is good practice for councils to appoint a Senior Information Risk Owner (SIRO) to help manage information risk, so we're pleased to see that 90% have created this role.

Local councils hold a lot of personal data across a wide range of services. Establishing an Information Asset Register (IAR) will help ensure a council knows what information it holds, where it is and which Information Asset Owner (IAO) is responsible for it. Yet our survey showed just 17% of councils has a complete IAR and 34% have yet to appoint IAOs.

The Local Public Services Data Handling Guidelines set out in more detail what information governance roles councils should have in place.

As well as keeping track of the information held, it's also important for councils to consistently monitor and benchmark their levels of compliance in order to facilitate continual improvement. This should be achieved through compliance reports and key performance indicators (KPIs) considered by a Corporate Information Governance Group (CIGG). Our survey found –31% of councils do not have a CIGG and 27% do not consider data protection training reports and KPIs.

Do council staff know what they need to know?

It's vital all staff keep data protection in mind – staff not knowing what they need to about data protection is behind many of the information security incidents our enforcement team sees in the local government sector.

Although the majority of councils told us they provide mandatory data protection training for staff processing personal data, we found it concerning that 18% of councils did not.

It's important councils remember to train temporary staff and provide annual refresher training for all staff. All the guidance on our website can be used for training, including our dedicated training resource area.

In the wake of an information security incident, swift reporting, containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals. As such, it's a good idea to have a proper incident management process. Yet our survey showed 14% of councils do not have an Information Security Incident Management Policy and 22% do not consider reports and KPIs for information security breaches.

The guidance highlighted in this blog is just a selection of help available from the ICO. Councils still need to be complying with the DPA in the run up to the implementation of GDPR. Adhering to good practice measures under DPA will stand organisations in good stead for the new regulations. We'll be updating the dedicated GDPR section of our website regularly with more information and guidance. The ICO also offers audits, a full index of guidance and a helpline service.

Thanks to all those who took part in the survey. You can view the full results of the survey here.