Scott-Moncrieff
business advisers and accountants

Are you GDPR compliant?

There's been a lot of talk about GDPR but here's what you need to know…

EU General Data Protection Regulation (GDPR) comes into force 25 May 2018.

The Information Commissioner's Office (ICO) currently enforces the Data Protection Act (DPA) and has powers to impose fines of up to £500,000. GDPR is a significant change to the law, and the ICO will be empowered to impose fines of up to 4% of global revenue or 20 million euros. GDPR encompasses all personal data held and processed either wholly or partly by automated means. This includes hard copy data if that data is part of a filing system or intended to become part of a filing system. Housing associations will be required to significantly update their policies to reflect changes between DPA and GDPR.

Significant changes to be aware of:

- The requirement to appoint a Data Protection Officer (for certain types of organisation);
- Changes to how consent can be obtained from data subjects for the use of their data. For example, data subjects have to explicitly 'opt in' to allowing their data to be shared, and it must be made clear what manner of data sharing they are opting into;
- GDPR introduces new rights for data subjects, such as data portability and the right to be forgotten, requiring housing associations to understand exactly where all data on a subject is held;
- GDPR is also clearer around the need to ensure that data held is being held for the purpose it was gathered and is being deleted when it is no longer needed for that purpose;
- Sanctions over sharing data outside the EEA will be strengthened. This requires organisations to ensure adequacy decisions or appropriate privacy safeguards are in place with organisations holding data outside the EEA. This impacts Cloud provision and outsourced services. These measures include Binding Corporate Rules and the use of the EU-US Privacy Shield.

In addition to the challenge of addressing the changes above, GDPR makes certain activities mandatory, for example:

- Providing new and existing staff with suitable training and awareness, as well as additional sources of guidance and support when required;
- Conducting Data Protection Impact Assessments (DPIA) in order to design data privacy into any new systems and processes. This is of particular importance if new technology is being deployed, where there is processing on a large scale of the special categories of data, or if profiling operations are being performed which are likely to have an impact on individuals;
- Notifying the ICO within 72 hours of a data breach;
- Holding those at executive management and board level accountable for compliance, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance.

Scott-Moncrieff
business advisers and accountants

What does this mean for housing associations like you?

Currently you will process information about your tenants in paper and/or electronic form. As well as general contact, tenancy and financial information this will include sensitive personal data, especially if you are involved in providing assisted housing for the elderly, vulnerable people or people living with a disability.

You might also share tenant data with building contractors and tenant survey agencies. In both cases, housing associations are still responsible for the safe keeping and privacy of tenant data.

It is important to be aware that the Scottish Government is also considering extending coverage of the Freedom of Information (Scotland) Act 2002 (FOISA) to Registered Social Landlords (RSLs), which will have further implications on how you manage information.

With some new elements, and significant enhancements, coming from GDPR it is essential you start planning for this now. Some changes will require new and updated procedures and will result in budgetary, IT, personnel, governance and communications implications for your organisation.

Recent breaches of data protection to learn from

You will have seen news headlines exposing breaches of data protection with eye-watering fines for the organisation at fault. GDPR means the scrutiny, and penalties, are set to intensify. Recent breaches include:

A housing association reported itself to the Information Commissioner after releasing tenants' private contact details.

Local Council fined £150,000 after publishing planning application documents online that included a family's health issues and personal details of all family members and the location of their home.

A double-glazing company fined £50,000 for making nuisance calls to people who had specifically stated they didn't want to be contacted.

Glasgow firm Xternal Property Renovations broke the law by making more than 109,000 calls to people registered with the Telephone Preference Service.

How we can help

Our GDPR assessment usually takes between one and two hours and could save you significant costs. We find that the assessment is most effectively administered in a workshop environment, where our team facilitate a self-assessment, present and explain the questions and the scoring system used. Their knowledge of GDPR helps participants explore, and challenge, participants' self-assessment and support consistency of interpretation across the different areas of the questionnaire.

We are helping a number of clients to ensure they are GDPR compliant.

We prepare for the workshop by holding an opening meeting to introduce you to the questionnaire and the scoring process. We also provide participants with guidance materials in advance to help them prepare for the workshop. After the workshop you receive a report showing your self-assessed maturity against the different areas of GDPR. We then work with you to develop an action plan to address areas of weakness.

Our team provides independent input and challenges both during, and after, the workshop to support you in considering all relevant aspects across your activities as a RSL and in interpreting the requirements of the GDPR.

Get in touch

Our team would love to speak with you further about GDPR and ensure you are in a strong position by May 2018.

Fraser Nicol
Partner, Glasgow
E fraser.nicol@scott-moncrieff.com
T 0141 567 4500

Liz McLean
IT Audit Manager, Glasgow
E elizabeth.mclean@scott-moncrieff.com
T 0141 567 4500