Do you know what data your Credit Union holds?

Board members and the management of Credit Unions can often underestimate the volume of member data that they hold. This may mean underestimating the potential impact and reach of the imminent General Data Protection Regulation (GDPR).

Where is your data?

If the Credit Union does not know what data it holds and where it is, the risk of non-compliance and exposure to subsequent penalty is increased. This is because the new rules which come into force in May 2018 introduce several new stipulations and repercussions for organisations that are not managing their data adequately whether it relates to members or employees.

Where did your data come from?

Organisations need to ensure that they are examining not only their primary records of member data (for example, your core banking and customer relationship management systems), but all data sources across all forms. Relevant data will be held in soft and hard formats.

It is imperative that you consider that your credit union may also hold personal or sensitive data relating to individuals who are not current members but to whom you have obligations under GDPR. This will include past members, but have you considered the data you hold re individuals who were unsuccessful in seeking membership? Similarly, during a loan application, you may acquire data relating to a person who holds a joint bank account with a member but is not a member in their own right.

Data can be generated or stored in the following locations:

- current IT applications;
- on the desktops of PCs;
- mobile phones and other devices;
- mobile data storage i.e. USBs and external hard drives;
- network folders;
- spreadsheets (and other such static documentation);
- emails and archived inboxes;
- other external communications;
- social media postings;
- microfiche;
- back-up tapes;
- filesharing platforms;
- web sites or online portals;
- decommissioned systems and IT hardware; and
- hard copy documents and archives.

These are just some examples to prompt your deliberations and planning. The implications of such varied storage scenarios are staggering when you consider the volume of data a Credit Union may hold.

RSM

Where do you go from here to prepare yourself against potential non-compliance?

A critical element of the GDPR readiness projects that all Credit Unions should now be conducting is an audit of all data sources across the entire organisation, so that reasonable steps can be taken to mitigate against the related risks which can arise.

Education of all staff will remain pivotal to continued compliance with these regulatory developments. Responsibility for maintaining the integrity of data cannot reside only with an IT department who maintain or support the core systems that hold data. Collective ownership of the data protection agenda must reach across all those departments that acquire, generate and use data.

If you have any questions or need further information please just get in touch.

Terry McAdam
Management Consulting Partner
+353 (0) 1 4965388
tmcadam@rsmireland.ie

www.rsmireland.ie