EIGHT STEPS TO MASTERING GDPR

Jeremy Twomey writes

Meeting General Data Protection Regulation (GDPR) compliance requirements has become a top priority for Irish businesses over recent months and accountancy practices are no different. Recognising that GDPR implementation presents both specific challenges and opportunities for accountants in practice, the Practice Consulting team has also been busy both offering advice and providing practical guidance in this area for our members.

This guidance can be found at https://www.charteredaccountants.ie/knowledge-centre/guidance/gdpr/gdpr-resources and includes the following:

- GDPR 8 Step Guide;
- Explanation of GDPR terms;
- GDPR Template Outline Procedures to be tailored and used by an accountancy firm; and
- Example paragraphs for a client engagement letter addressing GDPR and a template privacy statement.

From talking with our members in practice over recent weeks, it is evident that practitioners are at different stages on their journey to GDPR compliance. While it may appear a daunting exercise at the outset, the process of becoming GDPR ready can be broken down into a few key practical steps. With this in mind, in this article, I am going to outline the key points to achieve GDPR implementation from our 8 Step Guide:

1. **Raise GDPR awareness**

As a starting point on your GDPR journey, the partners and staff at your firm need to be fully aware of the Regulation, the work to be undertaken to ensure compliance, the likely problems that may arise and any budgetary implications. A basic step that can be undertaken in-house at your firm is a GDPR awareness presentation for all the staff.

Your clients also have to comply with GDPR, so it is worthwhile checking that they are aware of these changes, to tell them of their GDPR obligations and how your processes may be changing. Such support may be an ‘added value’ opportunity for your firm to assist your clients.
2. Appoint someone senior to oversee the process & resource this appropriately

Your firm should appoint someone internally to take control of understanding GDPR and how it will affect your practice. It is essential that this a senior member of staff who will take responsibility for overseeing the GDPR compliance process at your firm. While it is expected that the majority of the work in relation to meeting the requirements of GDPR can be undertaken internally, a project team may be required, which may include external support and assistance on certain issues. Hence, it is vital that reasonable funding and resources are set aside to achieve your GDPR requirements. It is currently envisaged that most accountancy firms will not be required to appoint a Data Protection Officer (DPO). It is, however, recommended that you still appoint someone to be responsible for data protection within the firm going forward, but give them a title other than DPO (i.e. “Data Privacy Lead”).

3. Review and update existing information and cyber security measures

Having comprehensive levels of information and cyber security is a key step towards building a resilient organisation and ensuring GDPR compliance. It is therefore recommended that members should review their existing security measures and update as necessary.

Both controllers and processors are required under the Regulation to implement “appropriate technical and organisational measures” to ensure a level of security appropriate to the risks that are presented by the processing of personal information. Such measures are described as including:

- Pseudonymisation and encryption of data (The use of secure portals to share documents is also of benefit);
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Detailed listings of examples of both practical physical and technical security measures to aid GDPR compliance at your firm are included in the full version of our 8 Step Guide as published on the Institute website. It is important to remember that managing cyber risk is not simply about managing data within your firm. Therefore, it becomes necessary to document the security risks from your supply chain (e.g. cloud service provider), as well as your own organisation.

4. Map your data

With the many potential pitfalls of non-compliance to GDPR, taking action to map any gaps in relation to the personal data your firm holds is critical. The first step is to get started by scoping the problem and mapping the data flows associated with your firm. It involves identifying, understanding and mapping out the data flows into and out of the organisation. As the data map evolves, you should be able to identify the flow of data, as well as gaps in required contracts and consents for processing data under the GDPR, and risks in security measures etc. that will need to be prioritised and resolved to ensure compliance.

This requirement for data mapping is quite far reaching when you think about it. A typical accountancy practice possesses the following: accounting and tax software, audit software, payroll software, practice management systems, network drives and, of course, paper accounting, tax, company secretarial and audit files. This review will also need to extend to the many individual devices on which information is stored (e.g. laptops, desktops, tablets, phones and memory sticks).

Finally, it is important to emphasise that, when completing your data mapping, GDPR compliance is only required for personal data that you hold. Company data is, for example, beyond the scope of the regulation, however your data mapping exercise may have an added benefit of identifying efficiencies that you can implement at your firm for non-personal data as well.

5. Review your contracts with clients and suppliers

As the GDPR imposes new obligations on data controllers and data processors, you will need to make sure you understand your status and your responsibilities with regard to both client data and firm data. At the very least, firm contracts will need to be updated to reflect the requirements of the GDPR.

Accountancy firms should review their existing contracts with their clients, suppliers and sub-contractors to identify whether the accountancy firm is the data controller or data processor of any personal data it processes under the different contracts. This involves identifying which party ultimately determines the purpose and means of processing data. It is of vital importance that you satisfy yourself that your firm is correctly assigned the role of either data controller or processor (with matching appropriate requirements/liabilities) before signing any contract with your client or supplier. Remember that entering into a contract on the wrong basis may potentially open both you and your firm to unnecessary requirements/liabilities that may be difficult to overturn.

More detailed guidance on each of these areas is included in the full 8 Step Guide, while Section 5 of our Outline Policies and Procedures provides advice on your firm’s
likely status as either a Data Controller or Processor for a variety of possible assignments that you may undertake. Both of these documents can be found on the Institute website under GDPR resources.

6. Employment contracts & information for your employees
As with existing legislation in this area, under GDPR, certain information must be supplied to employees before their personal data is collected and processed by your firm. The information will typically be provided in the form of a notice to job candidates, and a further privacy policy will be supplied to successful job applicants as part of their on-boarding induction to the firm (typically included in an Employee Handbook along with other firm policies).
It is also important to remember that, for the processing of employees’ personal data, where possible, the employer should rely on performance of the employment contract as the legal basis for processing, rather than consent. Consent is a weaker legal basis for such processing, as it can for example be easily withdrawn by the data subject. Finally, do not forget to review (and redraft as necessary) employment contracts to update any data protection references or sections to comply with GDPR.

7. Draft/update data protection policies and controls to meet the new requirements
The GDPR introduces the principle of ‘accountability’. This means that all organisations must not only ensure they are compliant with the GDPR, but be in a position to prove this too. The best way to prove this is to document your data protection policies and procedures. We suggest that your firm’s GDPR policies and procedures should include, but not be limited to, the following (Outline policies in several of these areas are included in “Outline GDPR Policies and Procedures” on our website):

a) Who is responsible for GDPR at your firm and what are the reporting lines?
b) Data Processing
Your policies in this area should detail the categories of personal data collected by your firm and the purpose for which it is collected. In addition, these policies should detail your firm’s role as a Data Controller and also instances when you act as a Data Processor, together with your responsibilities in fulfilling these roles.
c) Data Subject Rights
Your firm will need to have specific policies and procedures in place to ensure the rights of your data subjects are upheld under GDPR and that you have adequate processes and resources to meet the requirements of the Regulation. Specific subject rights requiring defined policies and procedures include:
• Data Subject Access Requests (DSARs);
• Right of erasure (Right to be forgotten);
• The right to restrict processing;
• The right to object to processing; and
• The right to data portability.
Some of these rights may not be enforceable by the data subject where data is held under legitimate purpose.
d) Data Governance
Example areas of data governance to be considered for inclusion in your GDPR related policies and procedures include the following: Data Protection Impact Assessments (DPIAs), Privacy by Design and Privacy Notices, Document Retention, Security and Breaches.

8. Staff training and ongoing compliance
While not all staff will need to understand the GDPR in its entirety at your firm, each of your staff should at least be aware that data protection is an issue for everyone. For staff who do not deal with personal data, training can be limited to an annual (refresher) course on information and cyber security. On the other hand, for staff who regularly deal with personal data, training should focus on security over data, plus an awareness of the firm GDPR policies and procedures on a regular basis (at a minimum annually or more often if the need arises). Again this can be tailored to their particular role and responsibilities.

Ongoing testing
Testing in the areas of IT Security and other key aspects of GDPR compliance (e.g. audits of records held for constant compliance) should be formalised into a regular ongoing programme of work at your firm, as well as outsourced providers. Cyber security is a rapidly evolving area. Meeting best practice in May 2018 does not mean you will maintain compliance over the months and years ahead; you will need to keep this area under review.

Conclusion
At first glance, the process to ensuring GDPR compliance may appear to be a massive undertaking and a drain on resources for your firm. It is important to bear in mind that most accountancy firms and small businesses are in the same boat as you, and that by breaking down the required steps into clear manageable stages as above, you too can achieve GDPR Compliance in a timely manner.

Should you need further assistance, Practice Consulting has also developed a half day consultation offering. One of our consultants can visit your firm and offer practical advice and guidance on how to tailor your procedures, make progress on your GDPR journey, and meet key compliance milestones. If you have any question in relation to GDPR, please feel free to contact either Conal Kennedy or myself in Practice Consulting.
The Chartered Accountants Ireland Tax Department writes:

REPUBLIC OF IRELAND TAX DEVELOPMENTS

Clarification on buyback of shares and trade benefit test

Revenue recently updated its Tax and Duty Manual, Part 06-09-01, to provide guidance on the application of the trade benefit test per section 176 of the Taxes Consolidation Act (TCA) 1997. This update supersedes previous guidance on the trade benefit test in Tax Briefing, Issue 25 (February 1997). In appendix II of the manual, Revenue set out examples where a share buyback would be considered to benefit the trade and consequently capital gains tax treatment would apply. The manual also provides technical guidance and illustrative examples on the tax treatment of share buybacks.

iXBRL: Mandatory use of Detailed Profit and Loss taxonomy

From 1 August 2018, Revenue’s updated Detailed Profit and Loss (DPL) taxonomy must be used for all iXBRL submissions relating to accounting periods ending on or after 1 January 2015. Also from 1 August 2018 Revenue will restrict the use of the IE GAAP and IE IFRS taxonomies. Section 110 companies are also subject to the mandatory use of the DPL taxonomy and restriction.

Revenue amended the following related iXBRL guidance sources as a result of the above changes:

- Tax and Duty Manual 41A-03-01
- Error Messages
- iXBRL FAQs
- iXBRL FAQs change doc v1.8
- iXBRL Style Guide

Links to these documents are available on www.revenue.ie and on the iXBRL knowledge centre of Chartered Accountants Ireland’s website.

NORTHERN IRELAND TAX DEVELOPMENTS

Making Tax Digital start date now under a year

Making Tax Digital (“MTD”) for VAT commences in under a year on 1 April 2019. From April 2019, only businesses with turnover above the VAT registration threshold (currently £85,000) will have to keep digital records, and only for VAT purposes. Download the Institute’s MTD for VAT decision tree (available on our website) and assess if your business or clients will be affected. Just a year after that on 1 April 2020, HMRC has stated that MTD for the other taxes will commence.

In April, HMRC launched the MTD pilot for Income Tax on GOV.UK. Agents can now set up an agent services account and sign up to use software to send income tax updates on behalf of their clients. Initially HMRC has opened the pilot to self-employed businesses with income from one business.

As HMRC develops the service, additional functionality will be added and gradually businesses with differing requirements will be allowed to join. In time, HMRC will make the pilot available to landlords with income from property and all self-employed businesses.

Agents can now:-

- Create an Agent Services account;
- Link existing SA client relationships to their Agent Services account;
- Sign up new and existing SA clients to quarterly updates;
- Submit updates through software – only applies when the agent is subscribed to agent services, the client is signed up to the MTD pilot for income tax, and the agent has enabled MTD compatible software for the client; and
- Be authorised by a new MTD SA client (a digital 64-8 for MTDB).

In addition, their clients will be able to:-

- Digitally confirm authorisation to the MTD pilot for income tax; and
- Digitally cancel authorisation for the MTD pilot for income tax.

HMRC is continuing to work closely with software developers who are providing software packages to support the MTD pilot. As the pilot progresses they will be making a wider range of new or updated software products available to agents and their clients.

In addition to the income tax pilot, HMRC launched the VAT pilot recently. Initially a small number of invited volunteers will test the service. As with the income tax pilot, HMRC will add functionality, continue to test and gradually allow businesses of differing types to join. You will be able to sign up your clients to the pilot before April 2019 when it becomes mandatory for those above the VAT threshold to keep digital records for VAT and send their VAT returns through MTD using software.

The Institute is launching its MTD hub on our website shortly. The hub will contain a number of resources aimed at helping members and businesses get MTD ready.
After significant engagement with the PSRA, the licence renewal forms have been updated for 2018 applications for renewals; these new forms were published on 9 April 2018.

The Bill transposes the 4th EU Anti-Money Laundering Directive into Irish law. The Bill has been published and will progress in due course through the houses of the Oireachtas. The Bill will transpose the 4th EU Anti-Money Laundering Directive into Irish law.

**Technical Alert 01/2018 Illustrative auditor’s report for the audit of financial statements prepared in accordance with the Micro Companies Regime of Companies Act 2014 and FRS 105 in the Republic of Ireland**

As you are aware, micro companies usually qualify for audit exemption under the Companies Act 2014; however, a company can lose its audit exemption where the company is late in filing its annual return. In these circumstances, and other cases where the directors of a micro company voluntarily decide to subject the financial statements to an audit, the auditor will need to be alert to the particular characteristics of forming an audit opinion in respect of financial statements prepared in accordance with the Micro Companies Regime of Companies Act 2014 and FRS 105. The Financial Reporting Standard applicable to the Micro-entities Regime.

One of the key differences between the financial reporting requirements for micro companies and those of other companies relates to the presumption, in law, of the financial statements giving a true and fair view when the minimum requirements specified by the Companies Act A 2014 are complied with. This Technical Alert highlights this and some of the other key issues in forming an audit opinion in relation to this compliance framework and also provides an illustrative auditor’s report.

**Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2018**

The Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill 2018 has been published and will progress in due course through the houses of the Oireachtas. The Bill transposes the 4th EU Anti-Money Laundering Directive into Irish law.

**PSRA licence renewal applications 2018**

In Practice Matter June 2017 we informed you of some changes to the Property Services Regulatory Authority (PSRA) licence renewal forms. The 2017 licence renewal forms required the submission of details of procedures in place or to be put in place by the licence holder in response to breaches of the regulations reported by the accountant. At the time we advised members that such details should be provided to the PSRA by the client under separate cover and not by the accountants in the appendices to the licence renewal application.

After significant engagement with the PSRA, the licence renewal forms have been updated for 2018 applications for renewals; these new forms were published on 9 April 2018. There are two renewal forms:

- **PSRA/L55 – Renewal ABC** where client accounts are held; and
- **PSRA/L55 - Renewal D** where service charges and/or sinking fund contributions are paid into a “relevant account”.


The licence renewal application now consists of two separate parts:

- Part I, Accountant’s Report is completed by the reporting accountant. The licensee’s role is to provide any documents requested by the accountant and to comply with

**IMPORTANT INFORMATION FOR FIRMS HOLDING INVESTMENT BUSINESS AUTHORISATION**

The Professional Standards Department writes
the accountant’s requests for documents and/or explanations relating to the accounting records. As in previous years, the accountant reports to the PSRA on the client account balancing statement at the year end. During the course of their work, the accountant may identify breaches of the regulations which fall to be reported to the PSRA in Appendix 1 Appendix 2 or Appendix 3B of their report.

- Part II, Licensee Submission is completed by the licensee. This is in two sections. Section 1 contains details of the person(s) listed on the bank mandate and their relationship with the licence holder. Section 2 details procedures that have been/ will be put in place by the licensee to address any breaches of the regulations which have been identified and reported by the accountant in Part I.

Scope of the accountant’s report

Members should note that Part II Licensee Submission is outside the scope of the opinion provided by the accountant. The accountant does not perform any work in relation to procedures identified by the licensee to address reported breaches and does not provide any assurance that those procedures are either appropriate to address the breaches or are properly implemented by the licensee. As we advised last year, if a member is requested by the client to assist in identifying or implementing such procedures, this work is undertaken as a separate engagement with separate engagement terms.

FRC has been designated as an Accounting Standard Setter under Companies Act 2014

The Financial Reporting Council (‘FRC’) has been designated as an Accounting Standard Setter under Irish law. As a result it will no longer be necessary for the Institute of Chartered Accountants in Ireland to act as the designated promulgator of the FRC’s financial reporting standards in Ireland. As such, references to accounting standards being “promulgated by the Institute of Chartered Accountants in Ireland” will no longer be necessary. This expression was used, for example, in the Financial Statements, when describing the financial reporting framework applied in their preparation, and in the Directors’ Responsibilities Statement included in the Annual Report.

In the past, the FRC’s Financial Reporting Standards have been given effect in Ireland by virtue of an agreement between the Department of Industry and Commerce (now the Department of Business, Enterprise and Innovation), the FRC and the Institute of Chartered Accountants in Ireland, such that the Institute would promulgate the FRC’s accounting standards in Ireland.

On 21 March 2018, the Minister for Business, Enterprise and Innovation signed the ‘Companies Act 2014 (Accounting Standards) (Prescribed Body) Regulations 2018’ which designate the FRC as “a body that issues statements of accounting standards” in Ireland (for the purposes of the definition of “accounting standards” in section 275(1) of the Companies Act 2014).

The Regulations came into operation on 28 March 2018, and are available on the Department of Business, Enterprise and Innovation website at the following link: https://dbei.gov.ie/en/Legislation/SI-No-84-of-2018.html

FRC issue March 2016 editions of accounting standards

The FRC has issued March 2018 editions of all UK and Ireland accounting standards. These editions reflect the triennial review amendments issued in December 2017, and other amendments made since the previous editions were issued. The March 2018 editions of the accounting standards also include the updated Republic of Ireland legal references appendices. The standards are available on the FRC website (https://www.frc.org.uk/news/march-2018/march-2018-editions-of-accounting-standards-reflec), and will be on CHARIOT in due course.

CPD COURSES FOR MEMBERS IN PRACTICE

Look out for our Going into Practice course, designed with you in mind, which is taking place in Dublin on 12 June and can be booked online through the Professional Development area of our website.

CONTACT POINTS

Practice Consulting (General)
E-mail practicemembers@charteredaccountants.ie
Fax + 353 -1- 5233 997
Telephone: Bernie Walsh + 353 -1- 6377 300

Practice Consulting Team
Conal Kennedy + 353 -1- 6377 396
Michael McAllister +353 -1-6377 252
Jeremy Twomey +353-1-5233 972

Queries, comments and suggestions are welcomed. The opinions expressed are solely those of the writers and not to be construed as those of the Institute. The purpose or technical articles is solely to draw the attention of the reader to issues, and these should never be construed as guidance or relied on. No liability is accepted by the Institute or the authors for persons acting or failing to act as a result of anything contained in this publication. © Copyright, Chartered Accountants Ireland.