Finín O'Brien
Solicitor, Ronan Daly Jermyn

Data Protection: How the GDPR Will Affect Chartered Tax Advisers

Introduction

Data protection has been to the fore of everyone's minds recently. News of cyber security attacks occurring on a weekly and sometimes daily basis, together with forthcoming considerably increased fines[1] for businesses, has raised concern. The General Data Protection Regulation (GDPR), a wide-ranging new piece of legislation, will change the way we deal with personal data. The GDPR will come into effect on 25 May 2018, and it builds on current Irish data protection legislation but also introduces new obligations and concepts. This article explains personal data and explores the main changes that will affect Chartered Tax Advisers (CTAs).

1 The current maximum fine is €100,000. This will increase under the GDPR to €20m, or 4% of the annual worldwide turnover of the data controller or data processor (whichever amount is higher).

What Is Data Protection?

Data protection is essentially the safeguarding of the privacy rights of living individuals. It should be borne in mind at all times that data protection legislation applies only to the use (i.e. the processing) of personal data. For CTAs, knowing exactly what comprises "personal data" is key to understanding data protection and, importantly, recognising when the legislation does and does not apply.

What Is Personal Data?

Personal data means "any information relating to an identified or identifiable natural person". In other words, personal data is any information relating to a living individual. This is a very broad definition by design. CTAs by their nature will hold a large amount of personal data. Examples include: individual client names and dates of birth; KYC (know your customer) and passport details; bank statements; family or beneficiary details; and client insurance information. CTAs will also hold personal data on their staff members, such as bank account details and PRSI data.

The following, however, would not be considered personal data:

- information relating to companies or corporate entities – i.e. information that does not contain personal details about an individual is not personal data;
- information where an individual cannot possibly be identified – anonymised data is not personal data; and
- information relating to a deceased person.

Further, and with the above kept in mind, data protection legislation applies only where personal data is:

- processed by "automated means", i.e. where it is processed on a computer; and/or
- processed in a "relevant filing system", i.e. hard copy data held in a filing cabinet.

What Are Data Controllers and Processors?

A data controller is a body that determines the purposes and means of the use of personal data. By contrast, a data processor simply processes personal data on behalf of a data controller. This means that data processors can use personal data only on the authority or instructions of a data controller. Examples of a data processor would be an external payroll operator or cloud service provider. As most CTA practices will be data controllers, they will be subject to data protection obligations and responsibilities.

Data Protection Principles

The GDPR is a principle-based piece of legislation. This means that the best way to summarise a CTA's data protection responsibilities is to examine the seven basic principles contained in the GDPR.

The good news, therefore, is that if CTAs follow and adhere to the principles below, they will be largely compliant with the GDPR:

- *Lawfulness, fairness and transparency:* personal data must be processed lawfully, fairly and in a transparent manner. It should be clear and transparent to an individual data subject what information is being collected by a CTA and for what purpose it is being used.
- *Purpose limitation:* personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. In short, an individual client or employee should not be surprised that a CTA is using his/her data in a particular way.
- *Data minimisation:* personal data must be adequate, relevant and limited to what is necessary. Personal data that are not needed should not be collected and should be deleted when no longer required.[2]

2 CTAs have specific legal requirements relating to the keeping of records. Sections 886 (Obligation to keep certain records) and 887 (Use of electronic data processing) of TCA 1997 provide that CTAs must hold certain information for at least six years. It should be remembered, however, that this is not an excuse to keep **all** personal data for this period. Other personal data that are no longer relevant should be deleted. For example, employee interview notes held after 12 months should be assessed for deletion.

- *Accuracy:* personal data must be accurate and, where necessary, kept up to date.
- *Storage limitation:* personal data must be kept in a form that permits identification of data subjects for no longer than is necessary.
- *Integrity and confidentiality:* personal data must be processed in a manner that ensures appropriate security of the personal data.
- *Accountability:* a CTA must be responsible for, and be able to demonstrate, compliance with all of the above principles. This is a new principle and effectively puts the onus on data controllers to show that they are compliant with their data protection obligations.

Legal Basis for Processing Data

A data controller may process personal data only when there exists a valid legal basis to perform such processing. Examples of a legal basis include: having the consent of the data subject; where the processing is necessary for the performance of a contract; or where the processing is necessary for the legitimate interests[3] pursued by the data controller. Legally, a data controller needs at least one legal basis for carrying out the processing of personal data. Ideally, a data controller would have more than one legal basis when processing data.

The grounds for processing personal data under the GDPR broadly replicate those under current data protection legislation. The main legal basis used by controllers is the consent of data subjects. Consent, however, will change under the GDPR. From 25 May 2018, all data controllers must ensure that if they are relying on the consent of a data subject to process personal data, then that consent must meet the higher standard set down in the GDPR.

Where relying on consent, a data controller must ensure that:

- the consent is freely given and the data subject provides an unambiguous indication that he/she consents – silence, inactivity or pre-ticked boxes will no longer be sufficient;
- consent is not "bundled" with other written agreements or declarations – it must be clear and distinguishable;
- data subjects are informed of their right to withdraw their consent at any time, and the method for withdrawing consent must be as simple as the method used for obtaining consent; and
- separate consents are obtained for distinct processing operations.

It is imperative that CTAs review the processing of personal data that they carry out and ensure that at least one legal basis can be relied on to justify the processing. If the legal basis is the consent of the data subject, then CTAs should ensure that this consent meets the higher GDPR standard.

What About Revenue Audits?

Revenue audits seek assurances that a business has filed true and correct tax returns based on the information contained in their underlying records. Some of this information may contain personal data, and a client may ask for advice about providing this to Revenue. Current data protection legislation[4] allows for personal data to be disclosed to a tax authority when it is required for the purpose of preventing or investigating offences or assessing or collecting any tax. The position under the GDPR will remain the same, as personal data can be

3 Except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4 Section 8 of the Data Protection Acts 1988 and 2003.

processed and disclosed when it is done in compliance with a legal obligation. A new Irish Data Protection Act[5] (clarifying certain areas of the GDPR) is due to come into force next year, and this may provide more specific details on this point. For the time being, Revenue published on 16 June 2017 a Manual on its data retention policy in relation to records obtained during a compliance intervention.[6] In addition, Finance Bill 2017 proposes the introduction a new section 851B to TCA 1997, affirming Revenue's data protection obligations as regards the processing and security of taxpayer information.

Fair Processing Notice

As under the current legislation, data controllers must provide transparent information to data subjects. This must be done at the time when the personal data are obtained. The information provided is commonly referred to as a "fair processing notice". Existing forms of fair processing notice will have to be re-examined as the requirements in the GDPR are much more detailed than those currently in place. This essentially means that more information will be required to be given to data subjects when obtaining their personal data. Data protection and privacy policies should be reviewed and updated where appropriate.

Data Protection Officers

A data controller is obliged to appoint a data protection officer (DPO) in three particular circumstances. None of the circumstances currently specified in the GDPR would readily apply to CTAs. So, although there may be no obligation to appoint a DPO, a CTA may still wish to do so. CTAs should approach this decision cautiously, however, because if a DPO is appointed, then all of the DPO requirements under the GDPR will apply. Examples of these requirements include the need for a DPO to be independent, sufficiently qualified and able to report to the highest level of management, and – most notably from an employment perspective – a DPO cannot be fired for performing his/her role.

What Rights Do Data Subjects Have?

Data subjects have certain rights under the current legislation. In recent years, these rights have become more widely known and utilised.

Below is list of rights that will exist under the GDPR:

- *Right to access data:* data subjects have a right to a copy of their personal data. The GDPR will change the time within which a data controller has to respond to a request from 40 days to one month. In addition, controllers will no longer be able to charge a fee[7] for responding to such requests: this will now have to be done free of charge.[8]
- *Right to rectification:* data subjects have the right to have any inaccurate personal data corrected by the data controller.
- *Right to erasure:* data subjects have the right have personal data deleted by a controller in certain circumstances.
- *Right to object:* data subjects have the right to object to certain processing activities of the data controller.
- *Right of restriction:* data subjects have the right to restrict or stop the processing of personal data in some situations.

5 The General Scheme of the Data Protection Bill 2017 was published on 12 May 2017. This is the first draft of the new Act.

6 See www.revenue.ie. Electronic and paper records provided in the course of compliance interventions are subject to the Revenue data protection policy and data protection legislation. See also Revenue's Code of Practice for Revenue Audit and Other Compliance Interventions, which states that all taxpayer information held by Revenue is confidential and may be disclosed only in accordance with s851A(2) TCA 1997 or as is otherwise provided for by any other statutory provision. In addition, Finance Bill 2017 proposes the introduction a new section 851B to TCA 1997, affirming Revenue's data protection obligations as regards the processing and security of taxpayer information.

7 Currently, the maximum fee that can be charged is €6.35. Although not a large amount, it can still act to dissuade access requests.

8 A data controller may be able to charge a reasonable fee if the request is manifestly unfounded, excessive or repetitive.

- *Automated decisions:* data subjects have rights in relation to decisions made by automated processes that significantly affect them.
- *Data portability:* this is a new right under the GDPR. It will allow data subjects to request that their personal data be transported from one data controller to another. This may occur in situations where a client wishes to change advisers and wants all of his/her personal data provided to a new adviser.

Data Processors

Data controllers must use only processors providing sufficient guarantees. This means that any relationship between a controller and processor must be governed by a contract in writing. This is currently required by Irish law, but the GDPR sets out in greater detail[9] what needs to be specified in the contract with a processor. CTAs should compile a list of all of their data processors (e.g. courier and shredding service providers) and review what contractual arrangement is currently in place and whether this arrangement will need to be updated.

Data Security

Taking into account the nature of the processing and costs of implementation, a data controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The GDPR builds on current obligations and provides some non-exhaustive examples of security measures:

- Implement "pseudonymisation" of data. This is the replacing of individual names with identifiers (e.g. client 54321). It can help to reduce the risk of someone being identified if a breach occurs.
- Encrypt personal data. If a controller loses personal data but the data cannot be accessed, then this will significantly reduce the security risk.
- Ensure the ongoing confidentiality and the integrity of processing systems.
- Be able to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident.
- Ensure that any person acting under the authority of the data controller processes data only on the instructions of the data controller.
- Regularly test, assess and evaluate all cyber security facilities. Perform false attacks and simulate drills.

Data Breaches: What to Do?

Although the best security measures can be put in place, data breaches can still occur. A personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". People often think that a data breach can occur only when external "hackers" get control of internal information. Although this scenario is important to avoid, the majority of data breaches occur when information is accidentally disclosed: for example, when client information is posted to the wrong client.

In the event of a data breach, the controller must "without undue delay" and, where feasible, not later than 72 hours after having become aware of it, notify the data breach to the Office of the Data Protection Commissioner (ODPC). Notification must be done unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The breach should also be recorded, detailing the facts relating to the incident, its effects and the remedial action taken. This is a big change from the current regime because, at present, there is no legal obligation to notify a data breach to the ODPC.

9 Article 28 of the GDPR sets out exactly what needs to be specified in a data processing contract.

From May 2018, there will also be an obligation to notify affected data subjects in certain situations. If a breach is likely to result in a high risk to the rights and freedoms of natural persons, it must be communicated[10] to the affected data subjects without undue delay. Again, this is a new feature of the GDPR. The potential consequences of this provision are evident, as the reputational damage that can be caused by data breaches can have significant adverse effects on a business.

Conclusion

Although the GDPR and the changes that it will bring may appear overwhelming at first, full compliance can be achieved if action is taken now. The best way to prepare is to understand fully the flows of personal data into and out of your business. This means understanding how personal data are collected and used and to where personal data might be sent. If you establish the flows of data throughout your company and apply the data protection principles set out above, it will allow you to advise your clients that their personal information is safe and secure with you.

Checklist

If GDPR preparation is on your radar, the following are some key takeaways to consider:

- ☐ *Establish a framework for accountability:* ensure that you have clear records and policies in place to prove that you meet the required standards. Establish a culture of monitoring, reviewing and assessing your data processing procedures, aiming to minimise data processing and retention and building in safeguards. Check that your staff are trained to understand their obligations.
- ☐ *Analyse the legal basis on which you use personal data:* consider what data processing you undertake and whether it is done by the consent of the data subject or on another basis. If you rely on consent, review whether your documents and forms of consent are adequate and check that consents are freely given, specific and informed. You will bear the burden of proof.
- ☐ *Check your privacy notices and policies:* the GDPR requires that information provided to data subjects should be in clear and plain language. Your policies should be transparent and made easily accessible to internal employees, external clients and, where appropriate, the public.
- ☐ *Bear in mind the rights of data subjects:* be prepared for data subjects to exercise their rights under the GDPR. Having proper and effective procedures in place to comply with, for example, data access requests will reduce costs in the long term.
- ☐ *Review your relationships with data processors:* consider whether the contractual documentation in place with your data processors is adequate and specifies all of the terms required under the GDPR.
- ☐ *Conduct an audit:* a gap analysis highlighting non-compliant areas is important to complete. Privacy impact assessments should be conducted to review any risky processing activities and set out the steps to be taken to address specific concerns.
- ☐ *Security:* a review of the security of all personal data should be undertaken. Any measures that can be implemented to bolster cyber security should be completed.
- ☐ *Prepare for data security breaches:* clear policies and well-practised procedures should be put in place to ensure that you can react quickly to any breach and notify the relevant parties in time where required. Have a team ready to deal with data breaches when they occur.

10 This should be communicated in clear and plain language and must describe the nature of the breach, the potential consequences and the proposed remedy.