Assessing Compliance with the General Data Protection

by Gerry Egan

In the previous article in this series (June 2019) I provided an overview of the GDPR and some of the key developments since it came into force on 25 May 2018. That overview has given rise to a number of requests for a compliance checklist that accountants could use in their own businesses and practices or when assessing clients' compliance. This article is designed to meet that requirement.

Bad news and good news

The bad news is that unlike accounting standards which have been developed over decades, there is no single standard that one can go to assess compliance with the GDPR.

On the other hand, the good news is that for SMEs and similar organisations, it is relatively straightforward to assess their compliance with GDPR once one has a good grasp of the key principles underlying the Regulation. The checklist that follows is one that I have developed based on experience of working with multiple medium-to-small organisations over the past two years in both assessing their state of compliance and helping them to close any gaps that we have identified.

The GDPR compliance checklist and how to use it

The GDPR Compliance Checklist is broken into three parts:

- Governance arrangements
- Adherence to key data protection principles
- Data subject rights

In the interests of space, the checklist is set out as a series of yes/no questions but in any assessment, there will be shades of grey e.g. an organisation may have a privacy notice, but it could be badly written or not easy to find on a website. Judgement on the part of the assessor is necessary to use the checklist effectively and deliver value for clients.

Governance arrangements

This section focuses on how the organisation is set up to manage its data protection obligations.

Board oversight

- Is the board aware of the organisation's data protection obligations?
- Does it have appropriate oversight arrangements e.g. receive regular reports on compliance progress, breaches, complaints?
- Has data protection been identified as a risk in the risk register?
- Has responsibility for GDPR compliance been assigned within the organisation?
- Has the board assessed whether it is obliged to appoint a Data Protection Officer and acted accordingly?

Responsibilities of Data Controller and Data Processor

The following responsibilities apply to all organisations:

- Have you identified all of the personal data and all of the categories of data subjects whose data you process, what business processes this data is used for and who you share it with?
- Have you established for which data you are a data controller i.e. make the decisions about the use of the data and for which data you are a data processor i.e. act on the instructions of others?
- Have you prepared appropriate privacy (fair processing) notice(s) and have these been communicated effectively to data subjects?
- Do you have a record of your data processing activities in your capacity as a controller, processor or both?
- Does the organisation understand its obligations in relation to identifying, recording and reporting data breaches and have arrangements in place for doing so?
- If you are a data controller. have you identified your data processors, and do you have appropriate contracts in place (vice versa if you are a processor)?
- Do you understand Data Subject Rights, and do you have a process to handle requests within one month of being received?
- Do you understand the circumstances in which it may be necessary to carry out Data Privacy Impact Assessments and have you done so?

The following additional responsibilities may apply to Data Controllers in certain circumstances:

- If you operate in more than one EU Member State, have you designated one Member State as the site of your Main Establishment?
- If you are based outside the EU, have you appointed a Nominated Representative to represent your interests in the EU? (only applicable to companies with no physical presence in the EU but included for completeness)
- If you control personal data jointly with another party, do you have a Joint Controller Agreement setting

out the respective responsibilities of the joint controllers?

- In addition to Joint Controllers and Data Processors do you share personal data with Recipients or other Third Parties and has the justification for doing so been documented?
- If you transfer personal data outside of the EU, do you understand and are you abiding by the rules governing such transfers?

Awareness and training

- Have you conducted appropriate training and awareness raising activities?

Policies

- Have you reviewed/updated/introduced relevant policies to ensure that they are GDPR compliant?

Adherence to Key Data Protection Principles

This section focuses on how well the organisation understands and adheres to the most important principles and how personal data is managed.

Transparency, Purpose and Lawful Processing condition

- Do you have a privacy notice, and have you communicated it effectively to Data Subjects?
- In relation to each category of data subject and set of personal data that you process have you identified the lawful purpose(s) for processing and which of the lawful processing conditions that you rely on, bearing in mind that different conditions apply to processing of 'ordinary' and 'special categories' of personal data?
- Have you recorded these details in your data processing record?

Purpose Limitation

- Are you using the data only for the purpose for which it was provided?
- If you propose to use the data for a different/additional purpose have you considered how you're going to communicate with the data subject?

Data Minimisation

- Have you taken steps to collect and process only the data that you require for the stated purpose?

Accuracy and Quality

- Have you taken steps to ensure the accuracy and quality of data and to keep it up to date?
- Are regular and systematic reviews undertaken to update personal data records?

Retention and Storage Limitation

- Have you determined how long you propose to retain different categories of data having regard to the principle that data should only be retained for as long as absolutely necessary?
- Do you have arrangements to systematically delete obsolete data at the end of the retention period?
- Are disposal methods appropriate?

Security and Confidentiality

- Have you considered the sources of risk to the privacy of the data subject both inside and from outside of the organisation?
- Are the technical and organisational security arrangements to protect the data e.g. physical security, IT security, appropriate access to records, commensurate with the sensitivity of the data and the risk to the privacy of the data subject?
- Is there an adequate focus on the confidentiality of personal data in your business practices?

Rights of Data Subjects

This final section of the checklist focuses on how the organisation protects the rights of data subjects and on how data subject requests are handled.

- Do you understand the rights of Data Subjects under GDPR?
- Do you have a documented process to handle requests within one month of being received?

And finally

Two final points: firstly, any assessment is only as good as the evidence presented. CPA members will be accustomed to asking, or being asked for, evidence of financial transactions as part of audits etc.

It is equally important when conducting an assessment of GDPR compliance to see the evidence.

Ask clients to: Show me your log of processing activities, demonstrate that data has been disposed of in accordance with your retention policy, illustrate how you have amended your application form to collect only necessary data.....

From the clients' point of view, it should be much more preferable for them to deal with tough questions from you rather than in the course of an investigation by the Data Protection Commission because of some non-compliance. If you or a client can answer in the affirmative to the above questions and support these affirmations with evidence, I would be confident that they are 'compliant with GDPR'.

Secondly, this checklist has been compiled for use in and by 'normal' businesses involved in selling goods and services, public sector organisations and non-profits. While the checklist is relevant in all cases some organisations have unique features like extensive use of automated decision making, complex international transfers of data or processing of children's data that may give rise to additional considerations that are not covered by this checklist. If any of these or other circumstances apply in your business, please feel free to contact the author for further guidance.

Gerry Egan,
M.Sc. (Mgmt.), C. Dir

Gerry is a Consultant and Trainer specialising in corporate governance, GDPR compliance and strategy working with clients in the private, public, and non-profit sectors.