BY
Hugh Jones

Hugh Jones is a co-founder of Sytorus Ltd, a specialised provider of Data Protection training, consultancy and assessment services. Hugh regularly advises groups of senior executives and strategic decision-makers eager to understand and comply with data management obligations.

Preparing for the GDPR – The 'Final Straight'

Hugh Jones provides a brief description of a number of elements which distinguish the GDPR from its predecessor (the 1995 EU Data Protection Directive) and to encourage organisations who have not yet done so to use the remaining weeks well.

Introduction

As we approach the impending deadline for the General Data Protection Regulation (GDPR), it might be helpful to focus on the key elements of the Regulation and to consider some actions on which members might concentrate in the coming few weeks (that is, those who have not used the past two years of lead-time to put the appropriate structures, policies and protocols in place!).

We are writing the paper from the perspective of CPA members, who are likely to be reading this in their capacity as Data Processors (third party service providers) and will (most admirably) be likely to have concerns for the GDPR compliance of their clients as much as their own compliance.

The GDPR comes into force on the same date, May 25th 2018, in each of the 28 EU member states. Compliance under the Regulation will be evaluated against seven principles, which will apply to any processing of personal data (data which identifies, either directly or indirectly) a living individual.

The Principles are:

1. That all processing of personal data should be fair, lawful and transparent.
2. That any processing of such data should only be for a specified and lawful purpose(s).
3. That only the minimum of processing of personal data will be conducted in order to achieve the purpose(s) – no excessive or unnecessary processing.
4. That, to the extent necessary, the personal data will be kept accurate and up to date.
5. That personal records will only be held for as long as required by relevant legislation and will then be destroyed, anonymised or returned to its source.
6. That throughout the time the data is held, the data will be kept safe and secure, adopting organisational and technological measures to do so.
7. That the organisation will implement the appropriate protocols, measures and policies to be able to demonstrate a commitment to GDPR compliance.

So what does this mean for Data Controllers (the organisations who determine the use of the personal data) and their Data Processors (third-party service providers)?

The following is a list of suggested areas for CPA members to focus on in the coming months – in no order of priority or importance.

Data Processor Agreements

As with the existing DP legislation, the GDPR requires that any third party service provider must operate within the terms of a formal, written contract in place between the Controller and the Processor – members should first and foremost ensure that they have a contract in place with their clients and that this contract makes specific reference to the member's obligations with regard to any personal data to which they might gain access during the course of their engagement with the client. The GDPR stipulates 12 clauses which must be referenced in this contract, details of which can be acquired from any advisor or from the web-site of the Irish DP Commissioner at www.DataProtection.ie

Process Logging

Organisations with in excess of 250 staff (both Controllers and Processors) must prepare a description of their main data processing activities, using headers stipulated in Article 28 of the Regulation – this document will serve as an initial indication to the ODPC, should they require it, of the ways in which personal data is acquired, shared, retained and disclosed by the organisation. The Process Activity Log should be available to the ODPC on request and therefore should ideally be drafted and 'ready to go' by May 25th.

Quality of Consent for direct marketing

Where organisations are relying on consent as the basis for their processing of personal data (perhaps for direct marketing or fund-raising purposes), they need to be aware that the criteria for consent have changed under the GDPR from May 25th 2018. Where organisations rely on consent, they need to be able to demonstrate that the consent was informed, freely given, specific

BY
Hugh Jones

and unambiguous and involved an active indication of the individual's preference. This last item will prove tricky, unless organisations have maintained a reliable record of how, when and under what circumstances the consent was acquired.

Organisations who cannot meet this standard will have time between now and May 25th to re-engage with their Data Subjects (whether they are customers/subscribers/donors/patients, etc.) and re-confirm their consent for such use of their data. The alternative will be to find an alternative lawful basis for such processing - a definitive list of which are set out in Article 6 of the Regulation for personal data and Article 9 for 'special categories of processing', such as the use of racial, ethnic, religious, political or medical information.

Obviously, the 'nuclear alternative' will be to cease processing of legacy data altogether and to start anew using the new criteria for consent. Some organisations have already done this but we don't recommend it unless all else has failed.

Privacy Impact Assessment

The GDPR will introduce a requirement that any proposed change to the way an organisation is processing personal data must be subject to an evaluation of the proposal – particularly where the proposed change might introduce such data to risk.

Known as a Privacy Impact Assessment (PIA), the review will require organisations to involve all relevant stakeholders and to consider the proposed change within the context of the seven principles outlined above. Any risk should be quantified and an appropriate risk mitigation measure should be implemented.

Given that members will regularly process personal data on behalf of their organisations, they will be likely be involved in many of these PIA's and in many cases, will be in a position to recommend to their clients when it is appropriate to conduct a PIA in the first place. For many clients, conducting a PIA may well be a new discipline and something our members can help them to understand.

As with the Processing Log, the output from the PIA should be documented and filed by the organisation for future reference. In the event that the proposed change leads to problems or complaints in the future, the ODPC is likely to request sight of a copy of the PIA Report as evidence that the organisation conducted an adequate risk assessment at the design stage of the project.

Breach Notification Reporting

The GDPR will require that organisations who have the misfortune to experience a Data Breach must notify the ODPC within a maximum 72 hours of becoming aware of the incident. A breach is defined as 'a (security incident) leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

In many cases, it may be the Data Processor who first becomes aware of the breach – in such circumstances, the obligation will be on them to inform the Data Controller as soon as possible.

The GDPR sets out some recommended items of information which should form part of the Breach Notification, including the nature and volume of the data compromised, the circumstances leading to the breach and the measures being taken to prevent a recurrence. The Controller must then work with the ODPC to respond to the breach in an appropriate manner – in some cases, this may require a communication to all Data Subjects impacted by the breach, informing them that their personal information has been exposed to risk.

Not a message any of us would relish having to compose and all the more reason to ensure that appropriate security measures are in place to prevent a breach in the first place!

Respect for Data Subject Rights

The GDPR will introduce some new rights for individuals, as well as reinforcing the rights which have already been in place since the 1995 Directive. The main difference is that there will now be an obligation on Controllers and Processors to respond to a Data Subject Right within no more than one month from receipt of the request. This will place a substantial burden on many organisations which were already struggling to meet the 40-day turnaround required in some circumstances under the current legislation.

Appointment of a Data Protection Officer (where required)

Much will be made in the media in the run-up to the GDPR launch date, of the requirement to appoint a Data Protection Officer (DPO).

The obligation only applies in certain cases – the GDPR sets out three circumstances under which the appointment of a DPO will be mandatory:

- where the Controller or Processor is a Public Body or Government Authority,
- where the organisation conducts surveillance of the public in a large scale, or
- where the organisation conducts special categories of processing, again in a large scale.

So the obligation to appoint a DPO will not apply in all cases. Even where it does apply, organisations will not have to hire a dedicated staff member for the role – the GDPR allows organisations to out-source the role or even to 'share' a DPO between several organisations or 'undertakings'.

Conclusion

We hope that this outline of the key provisions of the GDPR offers some guidance on areas for focus in the coming weeks. For those who miss the May 25th deadline, you will not be alone – many organisations have come late to the game and will continue in their efforts to be compliant long after May has come and gone.

What is most important is that organisations start somewhere, and our members are well-placed to advise and encourage them to achieve and maintain compliance.

If members require any support or guidance in their GDPR preparations, CPA Ireland is happy to team with Sytorus, a Dublin-based Data Protection consultancy, who can be contacted at info@sytorus.com, or at telephone number +353 1 683 3312.