MASON HAYES & CURRAN

iab ireland

GDPR

10 Actions to take now

The General Data Protection Regulation (GDPR) will come into effect on 25 May 2018. It introduces a number of significant changes in relation to managing personal data.

Highlights include:

- increased obligations around consent
- greater transparency requirements for privacy notices
- new security rules and breach reporting obligations
- a revamped regime for enforcement, remedies and liability
- the introduction of the principles of privacy by design and default.

Once the GDPR becomes law, the majority of its provisions will apply immediately across all EU Member States, including Ireland. This means that organisations cannot wait until after 25 May 2018 to rectify issues or implement changes. Businesses need to prepare now for the introduction of the new law.

IAB Ireland wants to help members understand what the new law means to their businesses and has partnered with member Mason Hayes & Curran to prepare this information leaflet on GDPR tailored to the digital advertising industry.

In this article you will find details on:

1. GDPR Awareness

Businesses and organisations should be aware that compliance and accountability are key concepts of the GDPR. As a result, to comply, organisations will need to review and possibly change processes and products.

For IAB members, the sooner you begin to prepare for the GDPR, the more cost-effective it is likely to be for your organisation. The GDPR gives data protection authorities more robust powers to tackle non-compliance, including the introduction of significant administrative fines of up to €20,000,000, or 4% of total annual global turnover, whichever is greater, for the most serious infringements.

The GDPR will apply to all organisations doing business in the EU, so make sure colleagues and employees overseas are involved and fully up to speed. Remember that the definition of personal data included in the GDPR covers more than personally identifiable information (PII).

Action

Key personnel should be made aware that the GDPR will affect your organisation and learn the steps to be taken to prepare for compliance. Appropriate training sessions should be given to employees involved in processing or management of personal data.

2. Becoming Accountable

Accountability under GDPR means that organisations must be able to demonstrate, and in most instances document, the manner in which they comply with data protection law in transacting business. It will be important to document all decision making in respect of data processing. Affected organisations will have to work on their internal compliance, including record keeping, and some may have to appoint a data protection officer (see Point 10).

As most of the requirements of the GDPR are interlinked and interdependent, GDPR-readiness should not be undertaken in a piecemeal fashion. Organisations should start a gap analysis of their existing data protection control environment against the new requirements. This exercise should, in detail, understand what personal data they have, why they have it, and who and where they transfer it to, particularly given the extraterritorial scope of the GDPR.

Data protection risk and compliance must become part of the organisation's DNA, in much the same way as general risk and compliance has become. In particular, for both new and existing products or services which involve the processing of personal data, organisations must ensure that the relevant product or service is designed with data protection compliance in mind. The concepts of data protection by design and default along with the requirement to conduct a Data Protection Impact Assessment in certain cases (see Point 8), suggest that data protection should be central to all change management projects in an organisation.

Action

Most organisations will likely, at a minimum, have to refresh their fair processing notices and rethink consent capture mechanisms. For many organisations, this will mean revising data protection wording on websites, online application forms, interactive voice recordings, call centre scripts, proposal and application forms, renewal notices and annual account statements.

3. Legal Basis for Processing Personal Data

For GDPR, organisations will have to identify the purpose(s) and the legal ground(s) for which they process personal data. Broadly, the GDPR offers six legal bases:

- Consent
- Contracts
- Legal compliance (with another law)
- Protecting the vital interests of a person
- Public interest
- Legitimate interest

IAB members should reflect on the ways in which they collect and process data and identify the purpose(s) for processing personal data and the legal basis or bases upon which to process

In digital advertising, and in other industries, organisations may seek to rely on consent and/or legitimate interests, as legal bases for processing personal data. Much will depend on what kind of processing you intend to do or whether you want to process the data for another purpose.

Action

Whatever the legal basis, organisations will have to document the purpose(s) and legal bases upon which they rely (see Point 3).

4. Consent

Consent plays an important role in the GDPR. However, consent is only one of six legal bases available to companies to process personal data, as set out above, and in some cases isn't the most appropriate legal basis.

If you are seeking to rely on an individual's consent to process their personal data, they must freely give specific, informed and unambiguous consent. This might include ticking a box when visiting your website. For example, under the GDPR, silence, pre-ticked boxes or inactivity will not constitute valid consent.

Consent should cover all processing activities carried out for the same purpose or purposes. So when the processing has multiple purposes, consent should be obtained for each of them.

The burden of proof under the GDPR lies with organisations to show that consent has been lawfully obtained. Organisations should review the systems by which they seek, obtain and record an individual's consent to ensure an effective audit trail, particularly if another organisation obtains consent on its behalf.

Action

Organisations should review agreements currently in place with their business partners to ensure they are in line with GDPR requirements.

5. Individuals' Privacy Rights

The GDPR strengthens the rights afforded to individuals of their personal data. Specifically, individuals must have the right to:

- be informed
- access to their data
- have inaccuracies corrected
- have information erased
- object to direct marketing
- restrict the processing of their information, including automated decision-making (see Article 29 Working Party draft guidance for more detail) and
- data portability (see Article 29 Working Party guidance for more detail).

Many of the rights individuals will enjoy under the GDPR are the same as those under current data protection laws but with some significant enhancements. Organisations who already comply with these principles should find the transition to the GDPR less difficult.

Action

Organisations should review and update processes to ensure they are in a position to adequately respond to any individual's access requests. There should be no undue delay in processing an access request and, at the latest they must be concluded within the newly prescribed time frame of one month.

6. Transparency and Privacy Notices

Transparency is one of the key data protection principles under the GDPR. It essentially requires communication of information to individuals about the collection and processing of their personal data in a simple, concise and easily accessible form, using clear and plain language.

Privacy policies, statements and notices are generally used to communicate information to individuals, which includes users and employees. Currently, data controllers must provide individuals with certain information about the processing of their personal data, including the identity of the data controller and the purpose for which their data is being processed.

The GDPR expands on this and requires data controllers to further inform individuals as to the legal basis being relied upon to collect their data, how long their data will be stored and of any data transfers to third countries. Individuals must also be informed of their right to make a data access request, to rectify or to delete their personal data. The GDPR requires different levels of detail depending on whether you obtain the data directly from the individual or not.

Action

It is a good idea to at this stage look at the privacy notices you currently use and consider what needs changing. It is never too soon to start making those changes if you haven't already.

7. Data Protection Impact Assessments and Privacy by Design and Privacy by Default

The GDPR seeks to ensure that the privacy rights of individuals are prioritised in a number of ways. The introduction of Data Protection Impact Assessment (DPIA) under the GDPR is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It will allow organisations to identify potential privacy issues before they arise.

The GDPR introduces mandatory DPIAs for organisations involved in processing that is likely to result in a high risk to the rights of individuals. For example, in instances where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals, or where there is large scale monitoring of a publicly accessible area.

The appropriate form of a DPIA will differ to suit each organisation. A DPIA can involve discussions with relevant parties/stakeholders.

The GDPR enshrines privacy "by design and default". Privacy by design requires data controllers to consider privacy measures and safeguards during product and service design processes in order to meet the requirements of the GDPR and protect the rights of individuals from the outset. Privacy by default requires data controllers to ensure that, by default, only necessary data is processed.

Action

IAB members that routinely process complex and large-scale personal data sets should consider preparing a DPIA questionnaire for the use of engineers, product teams, compliance team and legal counsel. In respect of privacy by design and privacy by default, carrying out a DPIA can help you assess how to incorporate these two principles into any new products or services you want to bring to market.

8. Data Breaches

Personal data breaches can have far reaching consequences, both in reputational and financial terms. You should therefore make sure you put in places processes that allow you to detect, report and investigate a breach.

The GDPR introduces mandatory reporting obligations on data controllers and data processors for data beaches.

If an organisation suffers a data breach, the GDPR requires a data controller to notify the local data protection authority, the Data Protection Commissioner in Ireland, without delay and where possible, within 72 hours. A data processor must notify the data controller as soon as the data processor becomes aware of a breach. Where the data breach poses a high risk to the privacy rights of individuals, affected individuals must also be notified without undue delay.

Failure to report a breach can result in a fine, as well as a fine for the breach itself. Organisations should review their current incident response plan and data breach management and reporting procedures for GDPR compliance (see Point 3). Check Article 29 Working Party draft guidance on breach notifications for more detail.

Action

Start now to identify those types of data that may trigger the notification requirement.

9. Data Protection Officers

For organisations whose core activities involve regular and systematic monitoring of individuals on a large scale, or involve processing large quantities of sensitive personal data, it will be mandatory to appoint a Data Protection Officer (DPO).

Action

If this applies to your organisation, then you will have to appoint someone with the responsibility for your GDPR compliance. You will also have to think where in the business structure and governance this person will fit in. For organisations that are unsure as to whether they need to appoint a DPO, the Article 29 Working Party recommends carrying out and documenting an assessment.

10. 'One-Stop-Shop'

One of the central pillars of the GDPR is the concept of the 'one-stop shop' which will assist those organisations which operate in many EU member states. Multinational organisations will be entitled to deal with one Data Protection Authority, referred to as a Lead Supervisory Authority (LSA) as their single regulating body in the country of their main establishment. For organisations whose main establishment is in Ireland, that will be the Data Protection Commissioner.

The main establishment of an organisation will typically be where the organisation has its central administration, where decisions about data processing are made, or where the main processing activities take place.

Action

Businesses and organisations should undertake a mapping exercise to establish where the central administration of the business is or where the significant decisions about data processing are made, as this will help to determine the main establishment and LSA.

About Mason Hayes & Curran

Mason Hayes & Curran has one of the foremost privacy law teams in Ireland, offering clients unparalleled global expertise coupled with detailed local knowledge. MHC's dedicated team of privacy lawyers provides world-class expertise and strategic advice on all issues surrounding data protection law to help organisations get ready for the GDPR.

About IAB

IAB Ireland is the trade association for digital advertising. As a member of the global IAB network IAB Ireland is the authoritative and objective source for all digital advertising issues whilst promoting best practise in the Irish digital advertising industry.

Key Contacts

Philip Nolan
Partner, Head of Commercial
Mason Hayes & Curran
+353 1 614 5078
pnolan@mhc.ie

Suzanne McElligott
CEO
IAB Ireland
+353 86 226 0403
suzanne@iabireland.ie