ARTHUR COX

Preparing for the GDPR

1 February 2018

EXPECT
EXCELLENCE

DUBLIN • BELFAST • LONDON • NEW YORK • SILICON VALLEY

arthurcox.com

The EU General Data Protection Regulation (known as the "**GDPR**") will replace the current Data Protection Directive 95/46/EC (the "**Directive**") from 25 May 2018. The purpose of the GDPR is to harmonise EU data privacy laws and to enhance the standard of data protection across all EU member states. Significantly, the GDPR will be directly effective in all EU member states without the need for any additional national legislation.

THE BASICS – 5 KEY GDPR QUESTIONS

1. **When does the GDPR take effect?**
   The GDPR enters into force on 25 May 2018 and will be directly effective in all EU Member States without the need for any further national legislation. However a Data Protection Bill is due to be enacted as part of Ireland's GDPR transposition.

2. **Does the GDPR apply outside the EU?**
   Yes. The GDPR applies to all data processing that takes place within the EU and where processing takes place outside the EU but the relevant controllers/processors are established in the EU. The GDPR also applies to data controllers and processors who either; (a) offer goods or services for free or payment (including advertising services); or (b) monitor the behaviour of data subjects located in the EU. Therefore the GDPR has a broad territorial scope and may apply to entities located in the US and elsewhere depending on their particular data processing activities.

3. **What is personal data?**
   The GDPR only applies where personal data is processed. The definition of personal data is broad under the GDPR but remains largely unchanged from the Directive. Personal data is defined as "*any information relating to an identified or identifiable natural person*". Any information outside this definition will not be subject to the GDPR. The GDPR specifically includes "*location data*", "*online identifiers*" such as IP addresses and "*genetic*" data as examples of personal data. Reinforcing the broad interpretation of personal data, the EU's highest court recently ruled that an exam script constitutes personal data. However, the GDPR does not apply to fully anonymised or aggregated data where a living individual cannot be identified.

   Sensitive categories of personal data attract a greater level of protection under the GDPR. These include: personal data relating to racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, health and biometric data, and data concerning sex life or sexual orientation.

4. **What is processing?**
   Again, data processing is a broad concept that includes a range of activities that relate to personal data including the collection, storage, recording, disclosure of, structuring, making available and erasure or destruction of personal data.

5. **Is my organisation a data controller?**
   The GDPR's obligations apply primarily to data controllers, defined as the entity that determines the purposes and means of data processing (either alone or together with others). If your organisation makes the decisions as to how and why personal data is processed it likely acts as a data controller. A processor is any entity which processes personal data on behalf of the controller.

KEY GDPR PRINCIPLES AND OBLIGATIONS

Principles of data processing

At the core of the GDPR are seven principles which must be observed by all data controllers and processors:

Principle 1 - Transparency

Transparency demands that data processing be undertaken in a transparent manner and data subjects are provided with certain information in relation to processing of their personal data.

Principle 2 - Purpose Limitation

Purpose Limitation is the principle that personal data is only processed for the particular purpose(s) for which it was collected (and for closely related purpose(s)).

Principle 3 - Data Minimisation

Data Minimisation demands that collection of personal data is limited to what is adequate, necessary and relevant to the purposes for which it was collected.

Principle 4 - Accuracy

The principle of **Accuracy** requires that personal data must be accurate and kept up to date and every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified.

Principle 5 - Storage Limitation

Under the principle of **Storage Limitation** personal data is not to be kept in an identifiable form for any longer than the purposes for which it was collected (subject to certain limited exceptions).

Principle 6 - Integrity and Confidentiality

The principle of **Integrity and Confidentiality** requires that technical and organisational security measures be put in place to ensure that personal data is protected from various forms of data breaches.

Principle 7 - Accountability

The seventh key principle is **Accountability**, which requires that data controllers are able to demonstrate compliance with each of their obligations under the GDPR.

Lawful bases of processing

The GDPR also requires that all data processing be supported by reference to one or more of the following grounds, which are known as "***lawful bases of processing***":

Consent

Personal data can be processed based on the data subject's specific, freely given and informed consent. However, the GDPR sets an elevated consent standard which requires that a valid consent must be provided by way of "*a statement or by a clear affirmative action*" and must be fully informed. Pre-ticked boxes and implied consent fall short of this standard. Significantly, data subjects must also have the right to withdraw their consent at any time and in an easy manner.

Legitimate Interests

Personal data may be processed based on the legitimate interests of the data controller (or a third party), including for advertising or marketing purposes. However, data subjects must be informed of the particular legitimate interest pursued and of their right to object to legitimate interest based processing. Such objection is then to be weighed against the controller's own legitimate interests.

Contractual Necessity

Personal data may be processed where necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering a contract. However such processing must be necessary to perform the contract.

Legal Obligations

Personal data may be processed where such processing is necessary to comply with legal obligations that are imposed on the data controller.

Other Lawful Bases

Other lawful bases include where processing is necessary in the ***vital interests*** of the data subject and where processing is necessary for the performance of a task carried out in the ***public interest*** or in the exercise of an ***official duty*** vested in the controller.

CONTRACTS WITH THIRD PARTIES

Data processing contracts – The GDPR lists certain mandatory clauses that must be included in all contracts between data controllers and processors that involve processing of personal data. Controllers should review all relevant contracts with processors to ensure that they meet the GDPR requirements.

GOVERNANCE

Data Protection Officer (DPO) – Certain organisations are required to appoint a DPO under the GDPR. These include: (a) public bodies; (b) controllers that engage in systematic monitoring of data subjects on a large scale; and (c) where the controller's core activity involves large scale processing of sensitive personal data. Many controllers and processors will not require the appointment of a DPO.

Record-keeping – The GDPR requires that controllers maintain records of their processing activities which must include details such as the relevant controller/processor, the purposes of processing and a general description of the categories of data subject and personal data processed. Other record-keeping obligations under the GDPR include the requirement to keep logs of data processors, records of any DPIAs and data breaches.

SECURITY

Security standards – Under the GDPR, both data controllers and processors are required to implement appropriate technical and organisational security standards appropriate to the risk of such processing. In assessing such risks the controllers and processors must assess the risk of accidental or unlawful loss, destruction, alteration, disclosure of, or access to personal data. In addition to security, controllers and processors must also ensure the resilience of and ability to restore data processing systems to ensure the integrity of and availability of access to personal data on an ongoing basis.

Technical and organisational measures – Without prescribing any particular security measures, the GDPR in particular encourages the use of **encryption** and **pseudonymisation**. Other security measures include access controls and physical security measures.

DATA BREACH NOTIFICATIONS

Data breaches – The GDPR defines a data breach as any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Data breaches may include hacking incidents, lost or stolen devices and, potentially, system failures which prevent access to personal data.

Compulsory breach reporting – The GDPR introduces a compulsory requirement for controllers to report data breaches to the relevant data protection supervisory authority (i.e. regulator) within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to data subjects. This determination requires that a risk assessment be undertaken.

Communication to data subjects – Where a data breach poses a high risk to data subjects, the GDPR requires data controllers to communicate the breach to the affected data subjects without undue delay. Again, this determination requires that a risk assessment be undertaken.

DATA TRANSFERS

Restrictions on data transfers – As with the current Directive, the GDPR restricts the transfer of personal data to locations outside the EU unless certain conditions or safeguards are in place. For example, personal data can be freely transferred to certain countries which the European Commission considers to provide an adequate standard of data protection. Otherwise, specific safeguards must be put in place to transfer personal data outside the EU.

Examples of such safeguards include so-called model contractual clauses and binding corporate rules. However, the landscape on data transfers is ever evolving in light of recent developments.

DATA SUBJECT RIGHTS

Under the GDPR data subjects are provided with certain enhanced rights in relation to their personal data. Controllers are required to respond to such requests free of charge and within 30 days of receipt of the request:

RIGHT OF ACCESS

The right of data subjects to obtain details concerning the processing of their personal data and to have access to a copy of any personal data that is processed.

DATA PORTABILITY

This is a new data subject right under the GDPR whereby data subjects may request controllers to provide them with the personal data that they have provided to the controller, including the right to have their personal data transferred to another controller (where technically feasible to do so). However, this right is subject to certain exceptions.

RIGHT OF ERASURE (THE "RIGHT TO BE FORGOTTEN")

Data subjects have the right to have their personal data erased without undue delay where certain conditions are met. However, this is not an absolute right and, for example, is not available where controllers are required by law to retain certain personal data or where it undermines the right to freedom of expression.

RIGHT OF RECTIFICATION

In line with the Accuracy principle, data subjects have the right to have any inaccurate personal data rectified without undue delay.

RIGHT TO OBJECT

Data subjects have a right to object to the processing, including profiling, of their personal data where such processing is based on legitimate interests of the controller (or a third party). Such objections may arise where personal data is processed or profiled for advertising purposes based on the legitimate interests of the controller (or a third party). In such a case, the controller must cease processing the data unless it can show that it has a compelling legitimate interest to continue such processing. The right to object is in essence a form of opt-out in relation to data processing for advertising/marketing purposes. The right to object also arises where personal data is processed based on public interest grounds.

NEW CONCEPTS UNDER THE GDPR

The following concepts have been introduced under the GDPR:

Pseudonymisation

Refers to processing of personal data in such a manner such that it cannot be used to identify a particular individual without having access to additional information. This requires that the additional information necessary to identify the data subject is kept separately and is subject to certain technical and organisational measures to ensure that the personal data cannot be used to identify a particular individual. Pseudonymisation essentially requires that the two datasets required to identify an individual be kept separately.

Profiling

Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

DPIAs

Data protection impact assessments or DPIAs are a new requirement under the GDPR in relation to processing activities that result in high risks to data subjects. DPIAs may be required particularly in relation to the roll-out of new technologies. Conducting a DPIA allows for an assessment of the risks that are inherent in the proposed processing activities, which in turn allows the data controller to identify and mitigate the risks before they commence the high risk processing activities.

Data Portability

This is a new data subject right under the GDPR whereby data subjects may request controllers to provide them with the personal data that they have provided to the controller, including the right to have their personal data transferred to another controller (where technically feasible to do so). However, this right is subject to certain exceptions.

Privacy-by-design

This is a new concept which requires that controllers effectively factor data protection principles into the product development, design and planning phases for new data processing systems in a manner that ensures GDPR compliance on implementation.

Privacy-by-default

This new concept requires that the default approach of data processing systems ensures compliance with certain data processing principles such as ***Data Minimisation*** and ***Purpose Limitation***.

ENFORCEMENT

The GDPR enforcement regime is significantly more developed than under the Directive and the data protection regulators (known as "**supervisory authorities**" under the GDPR) have wide-ranging powers and can impose substantial sanctions for breaches of the GDPR:

FINES

Supervisory authorities are empowered to impose fines that are "*effective, proportionate and dissuasive*", which may, depending on the particular breach, potentially represent the higher of €20 million or 4% of the relevant undertaking's worldwide annual turnover for the previous financial year. The use of the term "undertaking" in the GDPR is intended to broaden the scope of the group on which the fine may be imposed.

ENFORCEMENT POWERS

In addition to the power to impose fines, the GDPR provides supervisory authorities with a range of other powers including but not limited to:

- carrying out investigations and audits, including ordering controllers or processors to provide access to information and personal data;
- gaining access to premises of controllers or processors (including any processing equipment or systems);
- ordering controllers or processors to comply with certain data subject requests and to bring their processing into compliance with the GDPR;
- ordering a controller to communicate a data breach to affected data subjects; and
- imposing temporary or definitive bans on data processing.

COMPENSATION

Data subjects also have a right to sue data controllers and/or processors for material or non-material damage arising from a breach of the GDPR and data subjects are entitled to receive "full and effective compensation" for damage they suffer. Controllers and processors may be held liable for breaches unless they can show that they are not in any way responsible for the event which gives rise to the damage. The GDPR also provides for certain types of not-for-profit representative bodies to take data protection claims on behalf of multiple data subjects (in a similar manner to a class action).

ONE-STOP-SHOP

Under the so-called "One-Stop-Shop" system, each controller (and processor) will be primarily regulated by a lead supervisory authority within the EU member state of their main establishment (i.e. the place where the effective decisions regarding the purposes and means of data processing are taken). For example, if your organisation's main establishment is in Ireland the Office of the Irish Data Protection Commissioner will act as your lead regulator for the purposes of the "One-Stop-Shop" system.

Controllers or processors that do not have any establishment within the EU, but who are subject to the GDPR because they offer goods or services to, or monitor the behaviour of, data subjects in the EU, are required to nominate a representative within the EU. This representative is to be established in one of the EU member states where data subjects are offered goods or services or whose behaviour is monitored.

5 KEY THEMES UNDER THE GDPR

1. **Enhanced Transparency**
   A key focus is on providing data subjects with greater information in connection with the processing of their data in a *concise, transparent, intelligible and easily accessible* manner. The GDPR lists certain information that must be provided at either the point of data collection (where collected directly from the data subject) or within one month (where the data is obtained from a third party). Such information must include, for example, details of the controller and the lawful basis of the processing.

2. **Increased Accountability**
   The GDPR places greater onus on both controllers and processors to be accountable for and to be able to demonstrate compliance. For example, controllers must be able to show if a data subject has provided their consent. This principle permeates through the GDPR and informs other controller record-keeping obligations under the GDPR. Data processors are also directly subject to certain accountability obligations under the GDPR.

3. **Risk-based Approach**
   The GDPR places a premium on identifying and assessing risks. Adopting a risk-focused approach is an efficient and effective way of approaching GDPR compliance that is supported by the text of the GDPR.

4. **Record-keeping and documentary requirements**
   The GDPR places certain governance and record-keeping obligations on controllers, such as maintaining copies of all DPIAs conducted, keeping records of data processing activities and the implementation of appropriate policies. However, GDPR compliance is not simply a box-ticking or paper-based exercise.

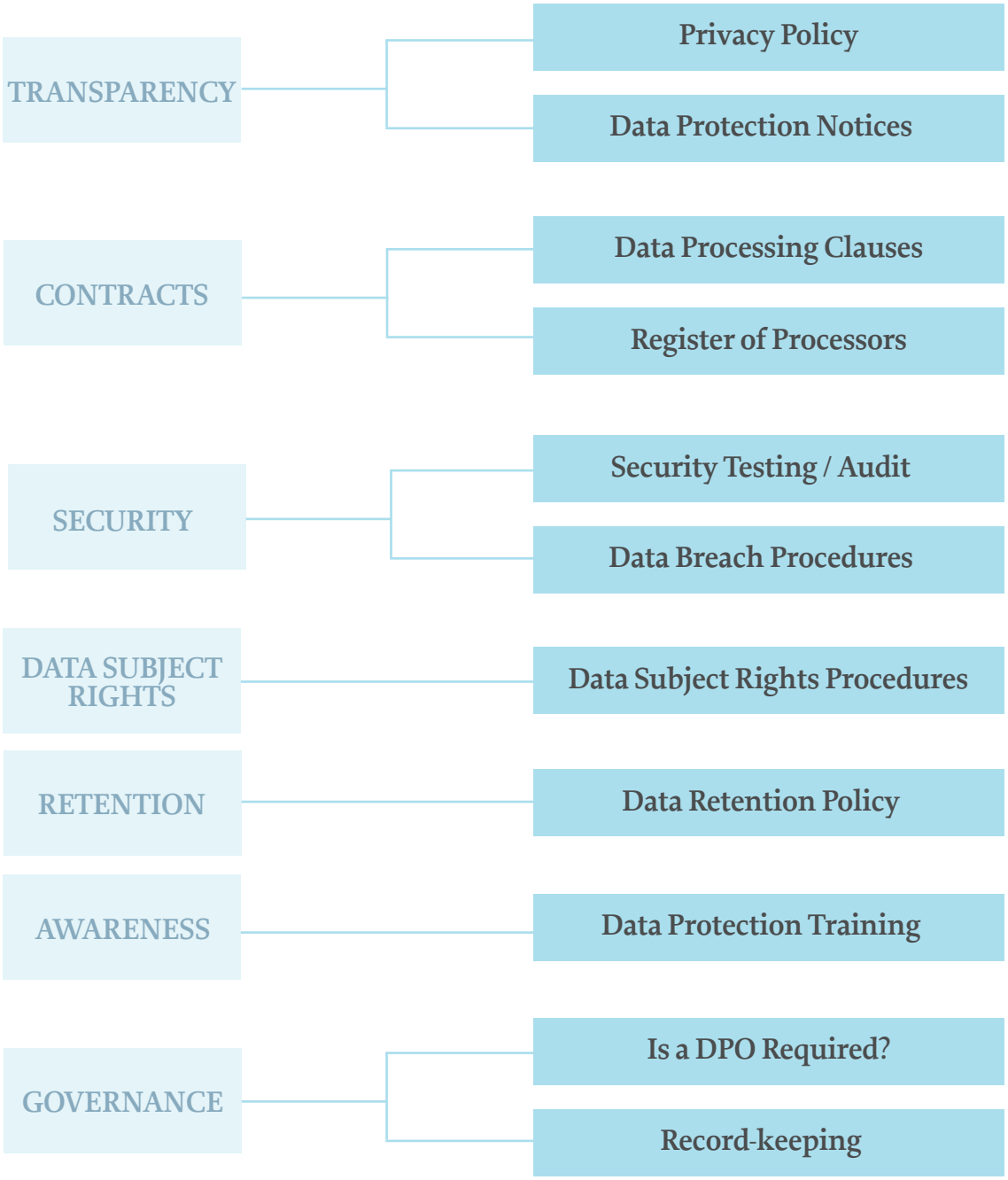
5. **Technical and organisational measures**
   While the record-keeping and documentation go some way toward GDPR compliance, they are no substitute for the implementation of technical and organisational measures to ensure practical compliance. These measures can range from simple physical solutions such as locking filing cabinets and limiting access to personal data, to more sophisticated IT security measures involving encryption and pseudonymisation.

"Accountability is the essence of the GDPR. Organisations... must be capable of demonstrating that accountability to data subjects and to regulators"

"The Article 30 obligation to document data processing operations is not a pen-pushing exercise. It's all about becoming aware. And compliance can only flow from awareness".

Commissioner Helen Dixon
Data Protection Commissioner for Ireland

GDPR COMPLIANCE PRIORITIES



"...the controller shall implement appropriate technical and organisational measures..."

Article 24, GDPR

THE ePRIVACY REGULATION

Overview of the proposed EU ePrivacy Regulation

In January 2017, the European Commission published its proposal for an ePrivacy Regulation ("**ePR**") to replace the existing ePrivacy Directive (Directive 2002/58/EC). The draft ePR is currently working its way through the EU legislative process with the most recent draft published in October 2017.

1. Timing

While the ePR was initially intended to come into force simultaneously with the GDPR, it is more likely that the ePR will be finalised in 2018 and enter force in late 2018 or early 2019.

2. Scope

The ePR will apply to all providers of electronic communications services including so called 'over-the-top' or OTT internet-based services (e.g. web-based email, voice-over IP and online messaging apps). Data-emitting connected devices will also be regulated by the ePR.

3. Extra-Territorial Effect

The ePR will have extra-territorial effect where services (including advertising) are provided to or target end-users located within the EU by providers located outside the EU, regardless of where the processing takes place.

4. Relationship with GDPR

The ePR is intended to "*particularise and complement*" the GDPR and also provides that "*electronic communications*" under the ePR will generally be considered personal data for GDPR purposes. In short, the ePR should be read in tandem with the GDPR as there is likely to be significant overlap.

5. Consent

The GDPR-level of consent will also apply under the ePR to the processing of message content and metadata for advertising purposes. This means that consent must be freely given, specific, informed and capable of withdrawal at any time. Unlike the GDPR, the ePR does not provide a legitimate interests ground for processing data.

6. Cookies

The ePR significantly alters the rules on cookies and other online trackers and use of such technologies must be based on an informed (GDPR standard) consent.

7. Consent and OBA

The ePR defines "*direct marketing communications*" to include any form of advertising in written, oral or video format which is "***sent, served or presented***" to end-users. This provision may have implications for online behavioural advertising given that prior consent is required to send or "*present*" direct marketing communications.

8. Enforcement

The ePR mirrors the GDPR with the potential fines of up to the higher of EUR 10 million or 2% of global annual turnover of EUR 20 million or 4% of global annual turnover, depending on the breach. The supervisory authority in each EU Member State responsible for enforcing the GDPR will also be responsible for ePR enforcement.

Note: this one page overview is based on the draft text of the ePR, which has not yet been finalised.

Meet Our Data Protection Team

This document provides a general overview of the GDPR but does not constitute legal advice. Please speak to your usual Arthur Cox contact or one of our team for further information:

ROB CORBET
HEAD OF TECHNOLOGY & INNOVATION
+353 1 920 1211
rob.corbet@arthurcox.com

COLIN ROONEY
PARTNER
+353 1 920 1194
colin.rooney@arthurcox.com

OLIVIA MULLOOLY
ASSOCIATE
+353 1 920 1060
olivia.mullooly@arthurcox.com

COLM MAGUIRE
ASSOCIATE
+353 1 920 1416
colm.maguire@arthurcox.com

HUGH MCCARTHY
ASSOCIATE
+353 1 920 1324
hugh.mccarthy@arthurcox.com

ANN-MARIE GLYNN
ASSOCIATE
+353 1 920 1081
ann-marie.glynn@arthurcox.com

CIARA ANDERSON
ASSOCIATE
+353 1 920 1347
ciara.anderson@arthurcox.com

Contact Us

Dublin
+353 1 920 1000
dublin@arthurcox.com

Belfast
+44 289 023 0007
belfast@arthurcox.com

London
+44 207 832 0200
london@arthurcox.com

New York
+1 212 782 3294
newyork@arthurcox.com

Silicon Valley
+1 650 943 2330
siliconvalley@arthurcox.com

arthurcox.com