ARTHUR COX

Group Briefing

February 2016

European General Data Protection Regulation Agreed – Headline Changes

KEY CONTACTS

ROB CORBET
HEAD OF TECHNOLOGY & INNOVATION
+353 1 618 0566
rob.corbet@arthurcox.com

COLIN ROONEY
PARTNER
+353 1 618 0543
colin.rooney@arthurcox.com

OLIVIA MULLOOLY
SENIOR ASSOCIATE
+353 1 618 1160
olivia.mullooly@arthurcox.com

On 15 December 2015, the EU institutions agreed the new data protection framework to be implemented under the forthcoming Data Protection Regulation. The European Parliament and European Council are expected to adopt the final text of the Regulation in the next few months and it will then come into effect two years after its adoption (likely mid 2018).

The Regulation will replace the current European legislative framework under the 1995 Data Protection Directive ("**Directive**") on which the primary Irish data protection law, the Data Protection Acts 1988 and 2003 (the "**Acts**") is based. The current system of various national laws, that transposed the Directive, resulted in a fragmented regulatory system for data controllers operating in the European Union. As the Regulation will have direct effect, it should allow for the application and enforcement of a more standardised data protection law across the EU. The reforms will also specifically address some current technological challenges and opportunities in respect of the processing of personal data in the current digital age, including profiling, data portability and the 'right to be forgotten'. However, many of the core principles around data processing in the Regulation remain unchanged from the Directive, but have been expanded and clarified to strengthen the rights of data subjects.

The following are some of the principal changes that will arise under the Regulation:

EXTRA-TERRITORIALITY OF THE REGULATION

Presently, any company which is established in the EU or which has equipment which is used to process personal data located inside the EU is subject to the Directive (as transposed into local law in the relevant EU country). Similarly, these companies shall be subject to the Regulation once that legal instrument is passed into law and becomes operative.

However, certain companies which were not previously subject to the data protection laws of a European Member State will come under the remit of the Regulation. This is because the Regulation will also apply to all businesses who are established outside the EU but who offer goods or services to EU residents (whether or not for payment), or who monitor the behaviour of EU residents, regardless of whether the processing takes place in the EU or not.

SUPERVISORY AUTHORITIES

Currently, each Member State of the EU has a national Data Protection Authority ("**DPA**"), i.e. in Ireland this is the Irish Office of the Data Protection Commission ("**DPC**"), and the DPC oversees the enforcement of the Acts.

Under the Regulation, each Member State will establish a Supervisory Authority ("**SA**") and it is likely that most countries will transition their DPA to be the SA for that Member State. The SAs will fulfil a similar role to that discharged by DPA under the Directive. Functions of the SA will include investigation and enforcement of the Regulation and co-operation with other Member State SAs. Furthermore, a data subject may complain directly to an SA, which will investigate such complaints.

"ONE STOP SHOP"

An important change that the Regulation introduces for multi-jurisdictional businesses is the concept of the "*one stop shop*" compliance framework. This mechanism is relevant to companies who operate across many jurisdictions.

In practice, the one stop shop may simplify interactions with data protection regulators as data controllers/companies will be subject to a "lead" SA (rather than having to interact with several different SAs simultaneously, as is presently the case). The competency of the lead SA will depend on which country is designated as the data controller's/company's "*main establishment*".

The lead SA will supervise the processing activities of the designated business throughout the EU and will consult and cooperate with the other national SAs (for example, in the context of international data transfers) in order to provide efficient and effective supervision of a business through one SA, rather than via multiple regulators.

CROSS-BORDER TRANSFERS OF PERSONAL DATA

From an Irish perspective and with reference to the Acts, the Regulation makes little practical impact on the requirements of businesses transferring data outside of the EEA.

Unlike the Directive, the Regulation will officially recognise Binding Corporate Rules ("**BCRs**") as a lawful method of data transfer for both data controllers and data processors within a group company structure or within "*groups of enterprises engaged in a joint economic activity*", where transfers to countries outside the EEA are envisaged. The Regulation will also simplify the process of adopting BCRs and provide a more streamlined approval process of BCRs on a cross-jurisdictional basis. The use of certifications and codes of conduct in the transfer of data are also addressed.

SEAL CERTIFICATIONS AND CODES OF CONDUCT

The Directive did not provide for the use of privacy seals or certifications which demonstrate to third parties that organisations are compliantly processing data. The Regulation recognises and encourages the use of privacy seals and certifications and adopts a framework for the use of such seals and certifications. The Regulation also allows for the submission of codes of conduct to the relevant SA for assessment in respect of compliance with the Regulation in this context.

INTERNAL RECORDS

Data controllers will be obliged under the Regulation to maintain internal records of data processing activities (which, in respect of content, will largely reflect the prescribed points already required to be addressed in a fair processing notice under Section 2D of the Acts as well as information on security measures and transfers to a third country). However, small and medium enterprises employing less than 250 persons need not keep such records, unless they process sensitive personal data or the processing they carry out is not occasional or likely to result in a risk for the rights and freedoms of data subjects.

DATA PROTECTION OFFICER

There will be an obligation on public authorities and bodies (save for courts acting in a judicial capacity) as well as data controllers and data processors whose core activities consist of processing operations "*which require regular and systematic monitoring of data subjects on a large scale*" or which consist of large scale processing of sensitive personal data to appoint a Data Protection Officer. This officer can be engaged as a consultant rather than as a full time employee.

REGISTRATION

The Regulation will abolish the requirement to register with data protection authorities.

NOTICE

There is a general principle in the Acts that certain information should be provided to data subjects detailing the processing of their personal data (i.e. an obligation to put the data subject on notice as to how their personal data is processed). The Regulation increases the amount of information to be included in such a notice.

One advantage to businesses of these notices is that a single notice should be sufficient for all Member States, albeit this notice will be much more detailed than was required under the Directive (as transposed). Interestingly the Regulation introduces a facility for the Commission to approve machine-readable standardised icons to assist data controllers in meeting their transparency obligations without having to rely on lengthy privacy notices.

DATA PROTECTION IMPACT ASSESSMENTS

Under the Regulation, businesses will be obliged to conduct Data Protection Impact Assessments ("**DPIA**") where the processing, particularly where it utilises any new technologies, "*is likely to result in a high risk*" for the rights of individuals, having regard to the "*nature, scope, context and purposes of the processing*".

The Regulation currently contains a non-exhaustive list of the situations in which a DPIA will be necessary, including where the data controller is monitoring publicly accessible areas or when sensitive personal

data is being processed on a large scale.

The principles of data protection by design and by default are also enshrined in the Regulation, whereby user settings will automatically be privacy friendly and the development of services and products will take account of privacy considerations from the outset.

PROCESSING LEGITIMATELY

Pursuant to the Directive and the Acts, there are a number of grounds with which to legitimise the processing of personal data, including obtaining the consent of the data subject and these have been largely unchanged by the Regulation. However, the scope of certain grounds has been addressed in further detail.

For example, in order to demonstrate the data subject's consent, a business will not be allowed to rely on pro-forma terms and conditions to do so, unless the request for consent is presented in a manner which is "*clearly distinguishable*" from the other matters, "*in an intelligible and easily accessible form, using clear and plain language*". Consent to the processing of sensitive personal data remains subject to the requirement that consent be explicit.

Any processing pursuant to a legal obligation on the data controller is also the subject of some attention in the Regulation, setting out some parameters as to how Member State or Union law may prescribe such processing.

Article 6 also sets out some guidance for determining whether data may be processed for another purpose other than that for which the data was collected.

RIGHTS OF DATA SUBJECT

As a general comment, the rights of the data subject are strengthened and broadened under the Regulation.

The rights of the data subject under the Regulation largely reflect the principles in the Directive and the Acts with the exception of two additional rights which will be granted to data subjects under the Regulation:

» the right to be forgotten (somewhat akin to the right arising from the Court of Justice of the European Union's ruling in *Costeja v Google*) whereby an individual may request the deletion of his or her data, provided that there are no legitimate grounds for retaining it; and

» the right of data portability enabling individuals to transfer their data to other service providers.

BREACH NOTIFICATIONS

There is currently no legislative obligation in the Acts for a data controller to report a data breach to either the DPC or data subjects. The Regulation will introduce an obligation to report all breaches to the SA within 72 hours (unless the breach is unlikely to result in a risk to the data subjects) as well as all high risk breaches to data subjects.

Practically speaking, this obligation will require businesses to establish a data breach response procedure. This requirement under the Regulation should also prompt an analysis of information security measures to ensure a robust security system is in place and that, for example, encryption of personal data is employed, where reasonable and practical.

PROFILING PROHIBITION

In the event that a business uses tools which process personal data in order to evaluate, analyse or predict a data subject's performance at work, economic situation, location, health, personal preferences, reliability or behaviour i.e. profiling, this will become regulated under the Regulation and only permitted in certain narrow circumstances, such as consent or pursuant to a legal right. The Regulation encourages the use of anonymisation, pseudonymisation and encryption for further processing of data (e.g. in data analytics).

ENFORCEMENT AND PENALTIES

The Regulation prescribes a harmonised sanctions regime for the EU by setting ranges of fines for administrative sanctions. The largest fine under the Regulation is currently the greater of €20 million or 4% of the annual worldwide turnover of a business. Under the Regulation, data subjects are also granted a judicial remedy against an SA to act on his or her complaint. This will likely mean that the SA is obliged to investigate every complaint made by a data subject. The latter will make little difference in Ireland as the DPC currently investigates all complaints made to it by data subjects. Data subjects will also be granted a judicial remedy against processors and controllers in respect of any processing of their personal data which infringes the Regulation.

SAs are also granted enforcement powers under the Regulation (i.e. to enforce compliance with the requirements of the Regulation) which the DPC did not have under the Acts and these powers are likely to increase the frequency with which sanctions are levied.

The risk of substantial fines, increased enforcement powers of SAs and grounds for seeking judicial remedies in the Regulation will mean that businesses in general will need to consistently monitor compliance with data protection law with heightened vigilance following the commencement into law of the Regulation.

IMPLEMENTATION

It is likely that the Regulation will be adopted in Spring 2016, to take effect two years thereafter, e.g. in mid-2018. Despite the attempt of the Regulation to harmonise data protection law throughout the EU, post its inception, it is likely that there will be some areas in which the Member States will be required to apply national law, e.g. employment laws.

FURTHER INFORMATION

For further information or specific advice regarding how the Regulation will impact your business, please contact any member of the Technology and Innovation team or your usual Arthur Cox contact:

JOHN MENTON
HEAD OF CORPORATE
+353 1 618 0558
john.menton@arthurcox.com

ROB CORBET
HEAD OF TECHNOLOGY & INNOVATION
+353 1 618 0566
rob.corbet@arthurcox.com

PEARSE RYAN
PARTNER
+353 1 618 0518
pearse.ryan@arthurcox.com

COLIN ROONEY
PARTNER
+353 1 618 0543
colin.rooney@arthurcox.com

ISEULT MANGAN
ASSOCIATE
+353 1 618 1153
iseult.mangan@arthurcox.com

OLIVIA MULLOOLY
ASSOCIATE
+353 1 618 1160
olivia.mullooly@arthurcox.com

CHRIS BOLLARD
ASSOCIATE
+353 1 618 0649
chris.bollard@arthurcox.com

CLAIRE O'BRIEN
ASSOCIATE
+353 1 618 1124
claire.obrien@arthurcox.com

JOANNE NEARY
ASSOCIATE
+353 1 618 1114
joanne.neary@arthurcox.com

COLM MAGUIRE
ASSOCIATE
+353 1 779 4356
colm.maguire@arthurcox.com