DATA PROTECTION IRELAND 2018 –BE PREPARED

JUNE 2018

On 25 May 2018 the new General Data Protection Regulation ("**GDPR**") came into force across the EU. This new regulation together with a new Irish Data Protection Act will have wide-ranging consequences for businesses and private individuals. Our article contains the main points and serves as a guideline for companies.

INTRODUCTION

1. How your personal data is dealt with?

"*Our automated systems analyse your content including emails to provide you personally relevant product features, such as customised search results, tailored advertising and spam and malware detection.*

….

*The information that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area (EEA). It may also be processed by our staff or by those of our suppliers***."**

Extract from the conditions of supply of services formerly used by Google

Blanket consents to exploit personal data such as this are longer acceptable.

2. Data Protection Legislation

The objective of legislation on data control is to adjust the perceived imbalance of rights and power relating to personal data between individuals that provide and organizations that receive and deal with that data in order to prevent the misuse and exploitation of that data. To achieve this objective, the basic principle of data protection, namely, that it is unlawful to process the personal data of another person unless a specific legal exemption (such as a statutory obligation, requirement to complete a contract, the existence of an appropriate consent or other legitimate purpose) applies.

3. Personal Data and Rights

"**Personal data**" means information relating to a living individual who can be identified either from the data, or from the data in conjunction with other information that is, or is likely to come into, the possession of a data controller.

The processing of the types of personal data (referred to as "**special categories of personal data**") revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health data concerning a natural person's sex life or sexual orientation is identified as requiring additional protection.

A "**data controller**" is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

If an organization simply holds or processes personal data on the instructions of another, but do not exercise responsibility for or control over the personal data, then it is a "**data processor**".

"**Processing**" in relating to personal data means performing any operation or set of operations on that data, including:

a) obtaining, recording or keeping data,
b) collecting, organising, storing, altering or adapting the data,
c) retrieving, consulting or using the data,
d) disclosing the information or data by transmitting, disseminating or otherwise making it available,
e) aligning, combining, blocking, erasing or destroying the data.

In short, virtually any use of or application in relation to personal data is processing.

4. Data Law Changes

From 25 May 2018, the EU General Data Protection Regulation (GDPR), became operative throughout the EU. It enhances legal obligations in relation to personal data. It also requires the creation of institutions in Member States to promote the highest standards of data security which must be followed by all organisations and will promote the creation of other institutions to assist individuals to ensure that data rights are respected.
By 25 May 2018, it is intended that all EU Member States will enact legislation to supplement the GDPR so that it can be fully operational.

5. The Data Protection Act 2018

As part of that EU wide exercise, a new Irish data protection Act (the DP Act) has been enacted. It replaces most previously enacted Irish data protection legislation.

6. Action required

If an organisation process personal data, then before 25 May 2018, in order to be ready to comply with the GDPR and the proposed new legislation, it should review, and if necessary, change its data practices to ensure compliance.

THE GDPR-ENHANCED PRINCIPLES

Enhanced principles of processing

From 25 May 2018, the controller must ensure that personal data which it controls is:

a) processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date, to the intent that every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
f) processed in a manner that ensures appropriate security of the personal data.

These requirements for data controllers on data processing are significantly more onerous that those that apply at present.

SUPERVISION, SCOPE AND FINES

1. European Data Protection Supervisor (EDPS)

The GDPR provides for the setting up of the EDPS. This is an independent EU body responsible for monitoring the application of data protection rules by EU institutions. Should the supervisory body in a Member State be considered to be remise in its data protection responsibilities, the EDPS can enforce compliance with the GDRP by taking the matter to the Court of Justice of the European Union "CJEU".

2. New Enforcement Authority for Ireland

After 25 May 2018, a new authority to be known as the Data Protection Commission will enforce data legislation in Ireland and will replace the existing office of the Data Protection Commissioner. Because Ireland has been chosen as a European base by many of the world's top data companies, Ireland is under pressure from its EU partners and the EU Commission to ensure compliance with the GDPR at every level. Clearly from the text of the DP Act, it is the intention of the Government that Ireland will carry out its obligations responsibly.

3. Who regulates a Controller located in more than one EU member State?

To avoid potential conflicts where an organisation is established in more than one EU Member State, the GDPR provides that the data protection authority in the Member State where the controller has its main establishment is to be the authority that regulates the data activities of that organisation. The main establishment of a controller in the EU is the place of its central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the EU, in which case, that other establishment should be considered to be the main establishment.

4. Increased Territorial Scope

From 25 May 2018, the GDPR will apply to any controller or processor which processes personal data in the context of its activities within the EU regardless of whether such activities take place in the EU or not.
The GDPR will also apply to non-EU companies dealing with personal data relating to the offering goods or services to persons in the EU, or monitoring individuals' behaviour in the EU.

Example
Codd Enterprises Inc., based in the US, sells computer games online worldwide. It has no establishment in the EU but 40% of its customers are based in the EU. It monitors the gaming activities of all of its

customers in a manner which allows them to be personally identified with a view to providing improved services. From 25 May 2018, Codd Enterprises Inc. will be subject to the GDPR. Depending on its circumstances, it may be obliged to appoint a data officer and/or a data representative.

5. Fines Increase

From 25 May 2018, an organisation which:

a) disregards the basic principles for personal data processing, including conditions for valid consent,
b) breaches data subjects' rights;
c) transfers personal data outside the EU without observing the GDPR requirements for security; or
d) commits another serious offence;

may be subject to an administrative fine of up to € 20,000,000, or in the case of a business, up to 4 % of total worldwide annual turnover in the preceding financial year, whichever is higher. Fines, for other infringements can be up to € 10,000,000, or in the case of a business, up to 2 % of total worldwide annual turnover of the preceding financial year, whichever is higher.

The DP Act provides for specific fines for other data protection offences. Under the DP Act, public bodies operating outside the commercial sphere will be exempt from administrative fines.

EU Member States are obliged to ensure that the imposition of fines for infractions of data protection legislation shall be effective, proportionate and dissuasive.
In addition to fines, where the rights of a data subject have been disregarded, damages and compensation may be awarded against the offending party.
Both EU organisations and non-EU organisations who fail to comply with data obligations under the GDPR are potentially exposed to enforcement and other proceeding.

The scale of the potential fines for infringements are so significant that it would be foolhardy not to take personal data compliance issues under the GDPR seriously.

DATA CONSENT

1. Requirements for Consent

From 25 May 2018, before a data controller who is relying on a consent to process personal data can process that data, the subject must have given consent to it in accordance with much stricter requirements than currently apply. From that date, the consent must be given:

a) freely,
b) specifically, for the purpose required,
c) the giver having been fully informed (long illegible privacy policies or statements full of legal jargon may be disregarded for information purposes), and
d) in an unambiguous indication of wishes

by a clear affirmative act such as by a written statement, including by electronic means, or an oral statement. Purported consent indicated by silence, pre-ticked boxes or inactivity will not constitute consent.
Consent is presumed not to be freely given (and therefore invalid) if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not otherwise being necessary for such performance.
Consent must cover all processing activities carried out for the same purpose or purposes.

Example
On 1 June 2018, Miss B has an industrial accident at work. She is obliged to take sick leave and makes a claim against her employer. To process the claim, the employer's insurer requires Miss B to attend a consultant neurologist and Miss B agrees to cooperate.
The claim is settled but as time passes, the relationship between Miss B and her employer deteriorate. The employer, who has a copy of the report of the consultant neurologist, uses information in it as grounds for dismissing Miss B. In consulting and using the report, the employer is data processing. Such usage in connection with the dismissal is unlawful under data protection law as there is no consent authorising it.

For a consent to be informed, the controller must notify the data subject of the facts in sufficient detail to enable the data subject to make a rational decision. The recommended principle which should be followed is the "no surprise" principle. This means that, on being informed afterwards about what his or her personal data has been used for, the expected reaction of the data subject should be one of no surprise.
At a minimum, the information to be supplied should include:

a) the controller's identity, all other organisations who will rely on the consent and where relevant any data representative,
b) the purpose of each of the processing operations for which consent is sought,
c) what (type of) data will be collected and used,
d) the existence of the right to withdraw consent,
e) whether the subject is obliged to provide the personal data or all of it and of the consequences, where he or she does not provide such data;
f) information about the use of the data for decisions based solely on automated processing, including whether any profiling will occur, and
g) if the consent relates to the data transfers, about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards.

The issue of consent must be dealt with in a way that clearly stands out or is in a separate document. If consent is requested by electronic means, the consent request has to be separate and distinct from other material provided.
The consequence of not complying with the requirements for informed consent is that the consent will be invalid.

Example

In June to September 2018, Y Co, a news organisation, obtains the consent of a large number of individuals who agree to respond to surveys by email to give their views and preferences in relation to political other events as they occur for. The individuals are informed that the answers that they give are to be used to help in reporting on newsworthy events and for such other purposes as Y Co may require. Unknown to the individuals, the information regarding their attitudes is also processed, analysed by Y Co and the data sold on to be used in connection with online marketing campaigns for companies selling goods and services. This additional use of the data by Y Co is unlawful and is a breach of the personal data rights of the individuals.
What Y Co should have done is to provide a specific form which in clear language invites each contact to consent to each individual process to which his or her data will be subject and providing a statement of the legal rights of that contract in relation to that data.

2. For how long is a consent valid?

A question that has not yet been satisfactorily resolved is for how long is a consent legally valid. The better view is that it will depend on what is reasonable in the circumstances. It has been suggested that where a data subject has given consent to receive direct marketing, the period should be short, perhaps not more than 2 years. Certain businesses have mentioned periods of 7 years in data policy statements which have been issued to customers.

3. Children and Consent

The GDPR creates an additional layer of protection where personal data of vulnerable natural persons, especially children, are processed. Article 8 introduces additional obligations to ensure an enhanced level of data protection of children in relation to information society services. This would include parental consent. The DP Act provides that 16 years is the age of consent.

4. What is the position where an organisation already has consents?

If an organisation currently process data and by 25 May 2018, does not have adequate consents for its processing of personal data, it must secure new consents or delete the data in respect of which consent for processing is incomplete or unavailable.

Example:
X Co is a travel agency founded in 1990 with files on clients who, in the past, availed of its services. The consents of the clients and former clients to receive emails were obtained using a set form with no opt out facility as regards receipt of emails. X Co regularly issues circulars to those clients and former clients inviting them to buy holidays. On 1 June 2018, X Co issues a holiday brochure to all clients on it data base. The mailing list includes individuals who did not use the services of X Co for more than 10 years.
On 1 July 2018 an inspector from the Data Commission visits the offices of X Co. Not being satisfied that X Co has the consents it is required to have, X Co receives a summons charging it with multiple data breaches.

OBLIGATIONS OF THE DATA CONTROLLER/PROCESSOR

1. To observe the General Principles of Data Protection

Obtaining consent does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, including, fairness, necessity and proportionality, as well as data quality.

2. Data Systems design requirement

A data controller must arrange that the system used for collecting and processing personal data is specifically designed to address the data protection rights of the data subjects whose data is collected both at the time of the determination, of the means for processing and at the time of the processing itself. This includes taking appropriate technical and organisational measures which are relevant in the circumstances, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the required safeguards.
A controller must ensure, in relation to personal data for which it is responsible, that an appropriate time limit is established for:

a) the erasure of the data, or
b) the carrying out of periodic reviews of the need for the retention of the data,

and ensure, by procedural measures, that the time limit is observed.
Staff must be trained and retrained, as necessary to deal appropriately with personal data issues.

3. A Controller must be able to demonstrate compliance with data legislation

A data controller must be in a position to demonstrate that it complies with all relevant data protection legislation and regularly reviews its activities to ensure continued compliance.
In relation to consents, it must be in a position to show that each consent was obtained lawfully and that the data subject was fully informed of the consequences. This means keeping records of all consents and may involve retaining records of website contents which are contemporaneous with the giving of the consent.
All personal data for which there is no record or an inadequate record of a consent must be deleted or the data must be rendered untraceable to the data subject from whom it was obtained.

4. Restriction on scope of processing personal data

The processing must be limited to what is necessary.

Example
Maxie, a builders' supplier, gives his customers the option to be sent an electronic invoice. He then stores the contact details and uses those details to send further emails to promote his business. What Maxie does with the personal data, beyond the issuing of the receipts, is illegal.

5. A Data Controller Cannot Retain personal data longer than necessary for the original purpose

Even if a data controller has consent to process personal data, that data cannot be retained indefinitely. The data controller must set time limits for erasure and for a periodic review.

Example:
In 2018/9, Z Co, a fitness club, keeps record of members and regularly emails those members regarding fitness and related opportunities at its fitness centre and other promotions. With the passage of time, members leave the club but nonetheless continue to be issued with mail from Z Co. In continuing to issue mail to lapsed members, and neglecting to erase their personal data after they have clearly ceased to be members, Z Co is acting unlawfully and its practice is in breach of the personal data rights of the individuals.

6. Security

A data controller must ensure appropriate security and confidentiality of the personal data collected, and preventing any unauthorised access to or use of that personal data and the equipment used for the processing it.

Example
ABC Bank outsources its data processing activities to DEF, a dedicated processor of data for financial institutions. In June 2018, the credit card data of some of the customers of ABC Bank retained by DEF were hacked and released on the internet. ABC Bank and DEF could face serious fines and claims from parties affected by the data breach.

7. Obligation to notify the Data Commission and affected Parties of Data Breach

A data breach is a breach of security in relation to personal data and includes an unlawful or accidental disclosure of personal data. After 25 May 2018, where a data breach occurs, the data controller must give formal notification (a breach notification) to the Data Commission. This must be done within 72 hours of the data controller first having become aware of the breach. The data controller must also describe the likely consequences of the personal data breach and state the measures taken or proposed to be taken to address the personal data breach. A data processor will also be required to notify the controller, "without undue delay" after first becoming aware of a data breach.
Where a data breach is likely to result in a risk for the rights and freedoms of individuals, the controller must notify the data subject of the personal data breach in plain language without undue delay.

8. To keep Records

A data controller must maintain a record of processing activities under its responsibility. That record must contain all of the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data; and

g) where possible, a general description of the technical and organisational security measures.

9. To have a Data Management Plan

A controller or processor must have a data management plan and to ensure that it is updated and complied. Failure to do so could result in fines, penalties and the obligation to pay damages for data breaches.

Example 1

In June 2018, Oliver, who worked in the human resources section of Bloggs' Supermarkets, in an act of spite against his employer, releases the personal data relating to 1,500 employees and former employees of Bloggs' Supermarkets Limited. In suffering this to happen, Bloggs' Supermarkets has committed a data breach. As soon as Bloggs' Supermarkets Limited becomes aware of the data breach, it must notify the breach of security in detail to the Data Commission and provide its offer of a remedy, otherwise it will commit a further data offence. It must also contact all those whose data have been compromised, take all reasonable steps to undo the consequences of the data breach and to the extent that they have suffered loss, compensate affected customers. Bloggs' Supermarket Limited is completely at sea. The consequences for it in loss of management time and adverse publicity are catastrophic for its business and it has the prospect of a series of legal claims against it taken by employees and former employees for many years to come.

Example 2

In June 2018, despite his data protection training, an unfortunate staff member of the PQR Hospital sends an email to a third party with an attachment containing sensitive personal data of 700 patients to the wrong person who promptly releases the information on the internet. Luckily, the PQR Hospital has a training and emergency data breach programme in place. Staff who have been trained for the purpose, spring into action in accordance with a prearranged plan. Whatever action to limit the damage caused that can be taken is taken immediately. Those affected are informed, receive a full apologies and counselling by trained staff in accordance with scripts have been ready in advance. A draft press release is available and the adverse publicity is contained.

Granted, the PQR Hospital must notify the Data Commission regarding the data breach and might incur a fine. However, the fact that it had significant resources in place to deal with the data breach should ensure that the adverse consequences are minimised.

10. To conduct data impact assessment in the case of automated (high risk) processing

Automated processing of personal data is to be subjected to a special stricter regime. For example of the requirements in this regime, before a data controller engages in processing activities using new technologies likely to result in high risk for the rights and freedoms of individuals the data controller must conduct an impact assessment and consult the relevant authorities.

RIGHTS OF THE DATA SUBJECT

1. Right of Access to and Correction of Data

A data subject has the right to inspect all personal data processed in relation to him/her. Once a formal application (a subject access request) is given to the controller, the controller must generally respond to it within a month, free of charge.

A data controller must ensure that personal data which are inaccurate are rectified or deleted.

Example
Henry is employed by the Blue Sky Roofing Company. In 2015, Henry was wrongly accused of fraud and threatened with dismissal. Having shown that he was innocent of the charges made against him, he requires the Blue Sky Roofing Company to allow him to inspect all of the data that the company has retained regarding the alleged incident and to either anonymise or destroy all record of the alleged incident the manner in which it was dealt with by the company.

2. Right to be forgotten

Subject to exceptions, a data subject will have the right to require a controller to erase personal data concerning him or her without undue delay where:

a) the data are no longer necessary in relation to the purposes for which they were collected
b) the data subject withdraws consent on which the processing is based,
c) there is no other legal ground for the processing;
d) the data subject objects to the processing and there are no overriding legitimate grounds for the processing; or
e) the personal data have been unlawfully processed.

Example:
In 2015, Cassidy, who lives in the town of Ballybog was convicted in the local court of being drunk and disorderly following New Year celebrations. The incident is reported in the Ballybog Chronicle, an online news sheet, and remains accessible for the public on a continuing basis. After a reasonable time, Cassidy will have the right to require the Ballybog Chronicle to remove the report.

3. Data Portability

From 25 May 2018, a data subject has the right to require the personal data retained by a controller transferred to another controller.

4. Right to have complaint addressed by the relevant authorities

If the data subject considers that the processing of personal data relating to him or her infringes the GDPR, he/she may lodge a complaint with the Data Commission. Where, in the view of the data subject the Data Commission does not handle the complaint properly or does not inform the data subject within three months on the progress or outcome of the complaint, the data subject may invoke the assistance of the EDPS. The EDPS may then bring the matter to the European Court to ensure compliance with the GDPR.

5. Right to Damages

With effect from 25 May 2018, any person who has suffered material or non-material damage as a result of an infringement of data rights shall have the right to receive compensation from the controller or processor at fault for the material and non-material damage suffered including emotional distress.

6. Right to assistance in a claim for data breach

Because, for an individual, the prospect of taking legal action in respect of a data breach could be challenging, the GDPR provides for a data subject to have the option to mandate a dedicated not-for-profit-organisation (to be set up in his or her jurisdiction for that purpose) to represent him or her in any claim. Under the DP Act, an award by a court in a case brought by a not-for-profit organisation may not include compensation for material or non-material damage suffered.

NEW OBLIGATORY POSTS OF RESPONSIBILITY FOR ORGANISATIONS

1. Obligation to employ a data protection officer

If a data controller or processor:

a) is a public authority or body, except for courts acting in their judicial capacity;
b) has core activities which consist of processing operations involving regular and systematic monitoring of data subjects on a large scale; or
c) is engaged in processing on a large scale of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data etc.) and personal data relating to criminal convictions and offences;

then it must appoint a data protection officer who is a person with expert knowledge of data protection law and practices.
This obligation applies not only to organisations established in the EU but also to organisations with no establishment in the EU where the personal data of persons in the EU is processed.

2. Obligation for non-EU Organisations to appoint a data representative

A controller or a processor not established in the EU which:

a) processes personal data of data subjects who are in the EU relating to the offering of goods or services to such data subjects in the EU, or
b) monitors their behaviour as far as their behaviour takes place in the EU,

must designate a data representative in the EU, unless the processing is occasional. This does not include the processing:

a) on a large scale, of special categories of personal data (sensitive personal data) or
b) of personal data relating to criminal convictions and offences, and is
    i. unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or
    ii. a non-EU established controller which is a public authority or body is exempt from this obligation.

Also, this obligation does not apply to an organisation employing fewer than 250 persons unless the processing it carries out:

a) is likely to result in a risk to the rights and freedoms of data subjects, is not occasional, or
b) includes special categories of data (race religion etc.) or personal data relating to criminal convictions and offences etc.

Example 1
Trojan Horse Inc., based in the US with less than 250 employees worldwide and with no establishment in the EU, processes data for health insurance companies in the EU. Its business dealing with health issues of data subjects in the EU comprises 20% of its worldwide business. Despite the fact that it only supplies services based on data which the insurance companies supply to it (under an appropriate security arrangement) and has no direct contact with data subjects in the EU, it must comply with the GDPR and that includes appointing a data representative.

Example 2
Fiji Fish Inc., based in the US with less than 250 employees worldwide, sells plastic fish on the internet. It does not directly market into the EU but keeps records of all customers and has valid consents where appropriate. Its business in the EU comprises less than 10% of its worldwide business. There is no need for a data representative. But nevertheless it is obliged to comply with the GDPR in so far as it relates to the rights of its EU customers.

The data representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under the GDPR.

The data representative must keep full records of data activities by its appointor.

The data representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority.

The designation of such a data representative does not affect the responsibility or liability of the controller or of the processor under the GDPR.

The data representative must perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with the GDPR.

The data representative must be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

To appoint a data representative will be a time consuming and very likely, a costly process. A non-EU controller or processor wishing to be compliant with the GDPR will be required to invest considerable time and resources in selecting and appointing a data representative.

3. Who can be a data representative?

A data representative can be a company, or an individual established in an EU Member State where at least some of the data subjects, being offered goods or services, or whose behaviour is monitored by or on behalf of the appointor, reside.

CONCLUSION

This article shows there are many issues to be addressed by a business that holds data about or markets to persons within the EU. To keep pace with the way the technology landscape has changed over the last decades, this legal update is overdue. As our data travels all over the world, it makes sense to unify the 28 disparate privacy laws of the EU Member States in two ways: to harmonize the law in the EU Member States but also at the same time to improve data protection on a worldwide basis, as companies outside the EU will be working on the personal data of EU subjects and therefore will be obliged to comply with European data protection laws. The GDPR is a big step towards a more cutting edge and unified privacy law.

For further information please do not hesitate to contact us.

URSULA TIPP
Partner
Tel: +353 1 254 3432
M: +353 86 1703405
utipp@tipp-mcknight.com

MICHAEL O'CONNOR
Partner
Tel: +353 1 254 3432
M: +353 86 8592838
moconnor@tipp-mcknight.com