GLOBAL
EXPERTS
LOCAL
SPECIALISTS

WE ARE
PHILIPLEE
WE'VE BEEN EXPECTING YOU

TOP 10 CHANGES INTRODUCED BY THE GDPR

philiplee.ie
info@philiplee.ie

DUBLIN
7/8 Wilton Terrace
Dublin 2
Ireland
T: +353 (0)1 237 3700
F: +353 (0)1 678 7794

BRUSSELS
39 Rue des Deux Eglises
1000 Brussels
Belgium
T: +32 (0) 2 640 3890
F: +32 (0) 2 648 2279

SAN FRANCISCO
201 Spear St.
Suite 1100
San Francisco
CA 94105
T: +1 415 213 2836

THE TOP 10 CHANGES INTRODUCED BY THE GDPR

THE GDPR – THE CHANGES TO DATA PROTECTION RULES, AND WHAT ORGANISATIONS SHOULD DO IN 2017 TO PREPARE FOR THEM (May 2017 – update with commentary on the Scheme of the Irish Data Protection Bill 2017)

The EU General Data Protection Regulation ("GDPR") was enacted on 24 May 2016 and will come into direct legal effect in all EU member states, including Ireland, on 25 May 2018. It replaces all EU member state general data protection rules. With some exceptions, the GDPR will operate as the new single data protection law for the EU. It is designed to give greater certainty to organisations in navigating and complying with data protection rules across all EU member states.

In many respects, after the GDPR, our Irish data protection rules will look and operate the same. Organisations will still require a specific legal basis for any processing of personal information that they carry out. They will still need to follow the eight data protection principles, including that they must be transparent with individuals about their data processing activities, they must ensure that the personal information they obtain and process is accurate and, where necessary, kept up to date, and they must keep personal information safe and secure.

However, the GDPR also introduces some significant changes to our current data protection rules. This note outlines the main changes to be introduced by the GDPR as they affect Irish-based organisations, and the steps that those organisations should take in 2017 to be ready for it coming into effect on 25 May 2018.

The GDPR will be supplemented by a new piece of national data protection legislation, the draft outline for which was published by the Department of Justice and Equality in May 2017.

In this note, we also comment on the contents of the outline (being the "General Scheme of the Data Protection Bill 2017") and the additional changes that it would introduce, if it is enacted as is.

1. SIGNIFICANT INCREASES IN SANCTIONS, THE INTRODUCTION OF ADMINISTRATIVE FINES IN IRELAND AND A RIGHT TO COMPENSATION FOR THE INDIVIDUAL

Currently, if an organisation breaches the general data protection rules, it can usually expect an aggrieved individual to complain to the Data Protection Commissioner ("DPC") or for the DPC to take action in relation to the breach directly. If the DPC ends up prosecuting the breach in the District Court, she can seek criminal fines of €3,000 per offence (as well as a custodial sentence and an Order for erasure of the relevant personal data). If the offence relates to direct marketing by electronic means (e.g. sending marketing text messages or emails without the proper consent), the DPC can seek fines of up to €5,000 per offence at District Court level. (The DPC will generally prosecute a number of sample offences, perhaps up to 10 or so.)

However, the GDPR significantly increases the sanctions that can be imposed for breaches of the data protection rules. At their highest, the fines can reach up to 4% of an organisation's annual worldwide turnover or up to €20 million. The GDPR sets out a number of factors that would need to be taken into account by national data protection regulators in deciding how serious the breach is, and therefore how far up the scale of fines the penalty should go.

In addition, the GDPR envisages that the sanctions can be imposed on public authorities or bodies by means of administrative fines. This would mean that the DPC would not need to prosecute a criminal case in the District Court in order to have a fine imposed on a public sector organisation for breaching data protection rules. The Data Protection Bill proposes to introduce a power for the DPC to impose administrative fines on public authorities or bodies arising from their activities as undertakings, i.e. in respect of economic activities in which they engage, usually in competition with the private sector, whereby they are regarded as undertakings for the purposes of competition law. In all other respects, it is proposed that the DPC will retain the ability to prosecute breaches on a criminal basis in the District Court.

The GDPR also introduces various means of redress for the individual whose data is misused, including a right of compensation for "material or non-material damage" or distress suffered by them. Whilst neither the GDPR nor the Data Protection Bill elaborate on what "non-material damage" means, it is likely to encompass damage for emotional distress caused by a data breach, something which is not necessarily compensated for under our current Irish rules.

What to do and how to prepare

The increased sanctions under the GDPR are designed so that organisations will treat their data protection obligations more seriously. They appear to be serving as the main motivating factor for organisations who are now examining their current compliance and whether and how they will be ready for the GDPR when it comes into effect.

Organisations need to now conduct something akin to a "gap analysis", looking at the increased compliance obligations that will fall upon them under the GDPR, where their compliance gaps are, what action they can/must take to remedy the deficiencies (including by means of putting in place policies, procedures and records, changing technology and changing business operations). They should also look to understand the risks to the organisation if they cannot become fully compliant by 25 May 2018.

2. INCREASED OBLIGATIONS OF TRANSPARENCY AND OTHER CHANGES TO THE DATA PROTECTION PRINCIPLES

The first data protection principle states that organisations must obtain and process personal information fairly and lawfully. A key component of meeting this obligation is that organisations must be transparent with individuals about their collection and use of the individual's personal information. The current legislation sets out a list of information that must be communicated to the individual in relation to the data processing, including about the identification of the organisation and its representative and the purposes of its data processing. There is a catch-all, information-neutral provision at the end, requiring the organisation to provide the individual with any other information that, having regard to all the circumstances, will make the processing fair. The DPC operates an unofficial rule of thumb on judging this transparency obligation – the "surprise test", the question being "would the individual be surprised by any of the uses that we are making of their personal information?" If the answer to the question is "yes", then the organisation will need to provide the individual with more information about their data processing activities.

The GDPR introduces a more detailed and longer list of information that organisations are required to communicate to individuals, in order to comply with the first data principle (now called the "lawfulness, fairness and transparency" principle). Included in this list are some confronting questions for organisations. For example, the requirement to identify the legal basis on which the organisation purports to process the personal information, the proposed retention period for the personal information (or at least the criteria used to determine the retention period) and detailed information for the individual about their data protection rights. The list differs depending on whether the organisation will source the information directly from the individual or from a third party.

The GDPR introduces a number of other key changes to the data protection principles, and which will serve to increase the compliance burden on organisations. Specifically, the data minimisation principle has been tightened. Currently, it requires that personal data that are collected and processed must be adequate, relevant and not excessive in relation to the purposes for which those data are collected and processed. The GDPR requires that the personal data must be adequate, relevant and "limited to what is necessary" in relation to the purposes for which those data are processed. This means that organisations must be strict with themselves about what data are necessary for them to process. If they collect and process data other than what are strictly necessary, they will breach the data minimisation principle.

In addition, the GDPR introduces a stricter "accountability" principle. The obligation under the current legislation is for the data controller to ensure compliance with the data protection principles. However, under the GDPR, the data controller is made responsible for, and must be able to demonstrate compliance with, the data protection principles. This obligation will need to read in conjunction with all of the increased compliance burdens imposed by the GDPR.

What to do and how to prepare

Generally, organisations will seek to meet their transparency obligations via communication of their data protection policies, and those policies will need to be updated in order to capture the additional information to be communicated. Organisations also need to understand that making available policies will not always be the most appropriate method of communication. Organisations need to examine the lists of transparency information they will be required to communicate under the GDPR (Articles 13 and 14 GDPR) and when they must communicate it, and then look carefully at their data collection points. They must understand precisely when and how they collect information from/about individuals and what their opportunities are for communicating the relevant information to the individuals at those points of contact. Organisations also need to satisfy themselves that the information is being communicated effectively, through clear language that is understandable to the intended audience.

In terms of the minimisation principle, organisations will need to critically examine the categories of personal information they collect and process, as against the purposes for that information use, and assess whether those categories of information are limited to what is strictly necessary in order to fulfil the relevant purposes.

3. NO REGISTRATION WITH THE DPC, BUT GREATER RECORD-KEEPING BURDENS

The current default rule is that all data controllers and processors must register themselves and summary details of their data processing activities with the DPC. This is subject to some exceptions. It is a criminal offence under Irish law to fail to register with the DPC where an obligation exists to do so. It is also an offence to process personal information where summary details of that processing have not been notified in the registration.

The GDPR removes the requirement for organisations to register with their national data protection supervisory authority. However, it introduces fairly onerous obligations to keep records of the data controller's processing activities, including:

- contact details;
- the documented purposes of the various data processing conducted by the controller;
- the categories of individuals whose personal information is processed and the personal information itself that is processed;
- the categories of recipients of the personal information;
- whether the personal information is transferred out of the EU and the safeguards which apply to protecting the information if it is transferred;
- the retention periods applicable to the information and (where possible) a description of the security measures applying to protect the information; and
- record-keeping obligations.

These record-keeping obligations will not apply to organisations employing less than 250 people, unless their processing activities are likely to result in a risk to the rights and freedoms of individuals, the processing is not occasional or the processing includes sensitive personal information (e.g. health-related information) or information relating to criminal convictions or offences.

In addition, Article 24(2) GDPR introduces an express legal obligation on data controllers to implement "appropriate data protection policies" where this is proportionate in relation to their data processing activities. Article 39(1)(b) GDPR underpins this obligation, by requiring the organisation's Data Protection Officer (where appointed) to police compliance with the data controller's policies.

What to do and how to prepare

Ideally, organisations should take the GDPR as a prompt to examine the personal data held by them and how that data flows through their organisation: where and how it is collected, stored and otherwise used, who is responsible for making decisions in relation to the data, what records are kept in relation to the data and what is the life cycle of the data through the organisation. They should keep records, not only documenting the personal data held, the purposes of the processing and the retention periods, but also the organisation's procedures for dealing with personal data, e.g. how information is collected over the phone and the information that should be communicated to individuals in telephone conversations and, for example, the procedures for dealing with requests by individuals to exercise their rights of access and other data rights.

Organisations should also take the opportunity to examine and update gaps in their data protection policies. Recommended policies include:

- General data protection policy
- Data security policy
- Data retention policy
- Email, internet, communications usage and monitoring
- Website privacy statement
- Cookies policy and related cookie notice for website
- Data breach policy
- CCTV policy and related CCTV notice

4. CONSENT: MORE DIFFICULT TO RELY ON CONSENT AS A LEGAL BASIS FOR PROCESSING, AND STRICTER RULES AROUND OBTAINING CONSENT

The GDPR makes it more difficult for organisations to rely on consent as a legal basis for their data processing. It introduces more hurdles around what constitutes a valid consent.

On its face, the definition of consent is not hugely different to the definition under current rules. The Data Protection Directive 1995 defines consent as any freely given, specific and informed indication of the data subject's wishes, by which the data subject signifies agreement to the processing of his/her personal information. The Directive goes on to require that the individual must have unambiguously given their consent. In similar terms, the GDPR defines consent as any freely given, specific, informed and unambiguous indication of the individual's agreement to the processing of his/her data. However, it goes on to state that consent must be given by a statement or a clear affirmative action. Coupled with an obligation under the GDPR that organisations must be able to prove that they obtained consent, this makes the burden of obtaining a valid consent more difficult.

The GDPR also confirms a number of other restrictions around organisations who might wish to rely on consent:

- ***Imbalanced relationships:*** Consent is unlikely to be regarded as "freely given" if the "consent" is from an employee to an employer, or from an individual to a public sector organisation. In addition, if the performance of a contract is made conditional on the individual consenting to processing activities that are not necessary for the performance of that contract, then the consent is also unlikely to be regarded as "freely given" – in other words, organisations cannot require individuals to give "consent" in return for obtaining a service.
- ***Unbundled:*** The GDPR also requires that the consent be "unbundled", i.e. kept separate from other terms and conditions or issues being communicated to the individual.
- ***Opt-in, not opt-out:*** The GDPR gravitates away from opt-out consent. It requires that consent is given by a statement or other clear affirmative action. Recital 32 of the GDPR clarifies that this could mean that a valid consent is provided verbally, in writing, by ticking a box or by choosing technical settings in an app. However, it also states that silence, pre-ticked boxes, failure to opt-out or other inactivity will not constitute a valid consent.
- ***Informed:*** The GDPR also requires that the consent wording should explain the nature of the intended processing of the personal information in an intelligible and easily-accessible form, using clear and plain language.
- ***Right of withdrawal:*** Consistent with a freely-given consent, individuals are given the express right under the GDPR to withdraw their consent at any time. They must be informed of their right to withdraw at the time of giving their consent, and it must be as easy for individuals to withdraw their consent as it was for them to give it. Happily, however, the GDPR does also clarify that withdrawal of consent will not affect the lawfulness of processing of the personal information that took place whilst the consent was still in place.

In addition, the GDPR makes clear that consents used or relied upon by organisations once the GDPR comes into effect on 25 May 2018 must be GDPR-level compliant consents. This means that the consents must meet all of the rules set out above. If they do not, then the organisation must obtain a new, GDPR-compliant consent. For many organisations, this will be a difficult if not impossible burden.

Finally, the GDPR makes specific provision for the obtaining of consent from children in relation to their participation in "information society services" (including in respect of them obtaining their own social media accounts). Article 8 GDPR requires that, where a child is below 16 years, the processing of the child's personal data will only be lawful in this context where their parent or guardian has consented. Information society service providers will have to make reasonable efforts to verify the parental or guardian consent. Member States are allowed to lower the applicable age to 13 years. The Data Protection Bill contains a draft provision on children's consent, but the Bill does not yet confirm whether Ireland will chose to lower the age from the GDPR-set threshold of 16 years.

What to do and how to prepare

Organisations need to examine:

- whether and to what extent they rely on consent as a basis for their personal data processing;
- given the changes under the GDPR, whether it is still appropriate to rely on consents, or should the organisation explore one of the other available legal bases under the GDPR;
- how they currently obtain those consents;
- whether those current consents would meet all of the new requirements, and be "GDPR-compliant" consents;
- if not, what does the organisation need to do to obtain GDPR-compliant consents, by 25 May 2018;
- how are consents recorded and/or how can the organisation prove that it has obtained consents?
- for information society services, how can the organisation verify the person's age, and, if parental or guardian consent is required, what mechanism(s) can the organisation put in place to obtain these and how can the organisation verify the parental or guardian consent?

5. APPOINTING AN INDEPENDENT DATA PROTECTION OFFICER

A key new obligation under the GDPR is the requirement that certain data controllers and processors appoint a Data Protection Officer (DPO). A DPO is an individual who takes responsibility for an organisation's data protection compliance. It is important that if required to do so, organisations have an appropriately qualified and effective DPO in place in advance of 25 May 2018.

It is mandatory for certain data controllers and processors to appoint a DPO, namely:

- Public Bodies (except for courts acting in their judicial capacity);
- Where the core activities of the data controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale (for example, operating a telecommunications network, data-driven marketing activities, location tracking, CCTV, connected devices); or
- Where the core activities of the controller or the processor consist of the processing on a large scale of special categories of personal data or personal data relating to criminal convictions and offences.

Even where the GDPR does not require the mandatory appointment of a DPO, the Article 29 Working Party (a group consisting of data protection regulators from all EU Member States, who issue influential guidance and opinions) has noted that organisations may sometimes find it useful to designate a DPO on a voluntary basis and in fact, the Article 29 Working Party encourages such voluntary efforts. However, it is important to note that when an organisation designates a DPO on a voluntary basis, the requirements under the GDPR relating to DPOs will apply as if the designation of the DPO was mandatory.

WHAT ARE THE TASKS OF THE DPO?

The DPO must carry out at least the following tasks:

1. Inform and advise the organisation (and any employees who process personal data) of the obligations under the GDPR and any other EU and national data protection law;
2. Monitor the organisation's compliance with the GDPR and any other EU and national data protection law
3. Monitor the organisation's compliance with their own data protection policies including the assignment of responsibilities, awareness training and training of staff involved in processing operations and the related audits;
4. Provide advice on the completion of data protection impact assessments and prior consultation with the supervisory authority; and
5. Cooperate with the supervisory authority and act as the point of contact for the supervisory authority.

WHAT QUALIFICATIONS & SKILLS MUST A DPO HAVE?

The DPO should be a professional with expert knowledge of data protection law and practice. The specific level of expert knowledge required should be determined according to the data processing operations carried out by the particular organisation and the protection required for that personal data.

For example, where an organisation processes a very large amount of sensitive personal data or systemically transfers personal data outside the European Union, the DPO must have a higher level of expertise.

The GDPR does not specify any particular qualifications which a DPO must hold. As minimum, the DPO must have expertise in national and European data protection laws and practices as well as an in-depth understanding of the GDPR. It is also useful if the DPO has knowledge of the particular business sector the organisation operates within. (IAPP offers a two-stage certification for DPOs, both ISO-certified, being their Certified Information Privacy Professional/Europe (CIPP/E) and their Certified Information Privacy Professional/Management (CIPP/M).)

The Article 29 Working Party have identified particular personal qualities, such as integrity and high professional ethics, that a DPO must have so he/she is able to fulfil the tasks required under the GDPR.

THE DPO'S ROLE IN THE ORGANISATION

Engaging a DPO

A DPO can be an employee or an outside consultant. It is not necessary that the DPO's sole/only function with the organisation is that of data protection. The GDPR acknowledges that a DPO may fulfil other tasks and duties within an organisation. However, if they do so, the other tasks and duties must not conflict with the DPO's role.

It is possible for a single DPO to be appointed across a corporate group. The GDPR provides that a group of undertakings may designate a single DPO so long as he/she is easily accessible from each establishment. Similarly, the GDPR permits a single DPO to be designated for several public bodies.

Publication of Contact Details

The contact details of the DPO must be published. This can be achieved by publishing a postal address, dedicated telephone number and/or email address where the DPO can be reached. Separately, the name and contact details of the DPO must be provided to the supervisory authority.

The objective of these publication requirements is to ensure that data subjects and supervisory authorities can easily contact the DPO directly in relation to issues regarding the processing of personal data.

Involvement in Organisation

One core issue is the position of the DPO within an organisation. The data controller and processor are obliged to ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protecting of personal data. The Article 29 Working Party recommends that this can be achieved by the organisation:

- Inviting the DPO to participate regularly in meetings of senior and middle management.
- Including the DPO in all decisions which have data protection implications, in particular, providing the DPO with all relevant information to allow him/her to consider the issue and provide adequate advice.
- Affording due weight to the opinion of the DPO. In cases of disagreement, the Article 29 Working Party recommends, as a good practice, that the organisation documents the reasons for not following the DPO's advice.
- Immediately contacting a DPO once a data breach or other data protection incident has occurred.

Necessary Resources

The organisation is obliged to provide the necessary resources to the DPO to carry out the tasks, access personal data and processing operations and maintain his or her expert knowledge. The level of resources required will depend upon the size of processing activities of the organisation.

The organisation should ensure that the DPO is provided with active support by senior management, is provided sufficient time to fulfil their tasks and provided sufficient resources (e.g. additional staff, infrastructure, financial resources) so he/she can fulfil their role.

Independence

The DPO must be independent. The data controller and processor cannot instruct the DPO as to how to conduct his/her tasks. Further, the DPO cannot be dismissed or penalised for performing his/her tasks.

What to do and how to prepare

IAPP conservatively estimate that 28,000 DPOs will need to be appointed across private sector organisations operating in the EU before May 2018. This does not take into account the separate requirements of public sector organisations to appoint DPOs and, indeed, the potential for non-EU based organisations to appoint them. There will be a race to identify and appoint suitably-qualified DPOs, and organisations need to assess now whether they need to appoint a DPO and if this is going to involve a full-time appointment, with the support of other privacy personnel and resources, or whether it can be part-time or indeed outsourced.

6. SPECIFIC DATA BREACH NOTIFICATION OBLIGATIONS

Although the DPC has approved a personal data security breach Code of Practice to help organisations react when they become aware of breaches of security involving customer or employee personal information, currently there is no specific legal obligation on organisations to notify the DPC or data subjects of a specific data breach. The one exception to this is providers of publicly available electronic communications networks or services who have specific data breach notification obligations under the ePrivacy Regulations.

The GDPR introduces mandatory reporting obligations on both data controllers and processors in the event of a personal data breach.

OBLIGATIONS ON DATA CONTROLLERS

Where there is a data breach, a data controller must report the data breach to the national supervisory authority. There is one exception where the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In general, we recommend that data controllers err on the side of caution and if in doubt whether the exception applies, adopt a policy that all data breaches are notified to the DPC.

Data controllers must notify the DPC of the breach without undue delay and typically within 72 hours after having become aware of the data breach. This is a tight timeframe which data controllers may have difficulty in complying with. At this stage, organisations should make sure that they have the right procedures in place to detect a data breach so the notification can be made as soon as possible to the DPC. If the notification is not made within 72 hours, the GDPR requires the data controller to explain the reasons for the delay.

The notification to the DPC must include, as a minimum, the following information:

- a description of the personal data breach including where possible, the categories and approximate number of individuals affected by the breach including the approximate number of personal data records concerned;
- the name and details of the DPO/other contact point within the organisation who the DPC can obtain information from;
- the likely consequences of the personal data breach; and
- the measures taken or proposed by the data controller to address the breach.

Data controllers are obliged to keep clear records relating to personal data breaches, including the facts relating to the data breach, its effects and any remedial action taken. These records must be disclosed to the DPC on demand.

Separately, breaches that are likely to bring harm to an individual – for example – identity theft or breach of confidentiality – must also be reported to the individual data subject. The GDPR does not impose a specific time frame to report such breaches to the individual and requires the notification is made "without undue delay". The notification to the data subject must include at least the following information:

- the name and details of the DPO/other contact point within the organisation who the DPC can obtain information from;
- the likely consequences of the personal data breach; and
- the measures taken or proposed by the data controller to address the breach.

It is not necessary for a data controller to notify data subjects of a personal data breach if one of the following conditions apply:

- technical and organisational protection measures taken by the data controller means that the personal data is now protected (for example, encryption);
- in light of measures taken by the controller (for example, suspending affected accounts), it is unlikely that the breach will bring harm to the individual; or
- it would involve a disproportionate effort (in such cases, the data controller is not absolved of the obligation to notify data subjects and the data controller must make a public notification of the data breach).

If a controller has not communicated a breach to data subjects, the DPC has the power to require the controller to do so.

The DPC recommends that data controllers now assess the types of data held and document which ones fall within the notification requirement to a data subject in the event of a breach. The DPC notes that larger organisations will need to develop policies and procedures for managing data breaches, both at central or local level. Data controllers will be aware of the huge reputational damage that can arise from a data breach. it will be important to have the necessary security measures and procedures in place to avoid data breaches and so that it is possible to act effectively and efficiently if a data breach in fact occurs.

In light of the significant penalties under the GDPR, it is important to remember that failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

OBLIGATIONS ON PROCESSORS

Where there is a data breach, the processor is obliged to notify the data controller. The GDPR does not include a specific time frame for such notification and requires that the notification is made without undue delay after becoming aware of a personal data breach. In order to ensure compliance with the GDPR, it is recommended that controllers review its current data processing agreements with processes to ensure that this notification obligation is reflected in the agreement. If the agreement does not include this obligation, it will need to be amended in advance of 25 May 2018.

Upon receipt of a data breach notification from a processor, the data controller will need to consider whether the reporting obligations (described above) apply.

7. ENHANCED RIGHTS FOR INDIVIDUALS, INCLUDING THE INTRODUCTION OF THE RIGHT TO DATA PORTABILITY

The GDPR expands the current body of rights provided to data subjects and creates a number of entirely new rights. Both data controller and processors must be aware of these enhanced rights for individuals and ensure that their procedures and policies give effect to these rights.

Importantly, the time for response to requests to exercise rights has been specified under the GDPR as (uniformly) one month. This will represent a challenge for organisations in being able to effectively and quickly respond to requests from individuals to exercise their rights, particularly where the organisation holds a large and diversely-located bank of data about the individual.

KEY RIGHTS FOR INDIVIDUALS UNDER THE GDPR

THE RIGHT TO DATA ACCESS	An individual will be entitled to be informed by an organisation whether the data processed by or on behalf of the organisation includes any personal data relating to the individual, and, subject to certain exemptions, obtain copies of such data. This is subject to the provision of a written data access request and payment of the appropriate fee by the individual. This right extends to personal data held in manual or automated form. Manual data, however, will only be subject to the GDPR if they form part of a "relevant filing system" i.e. where the personal data is stored in such a way that specific information relating to an identifiable individual is readily accessible.
THE RIGHT TO RECTIFICATION	The right to rectification arises where personal data held by an organisation is inaccurate or incomplete. An individual will be entitled to obtain from the organisation the rectification of inaccuracies in personal data held about them. If personal data held about the individual are incomplete; an individual can require the organisation to complete the data, or to record a supplementary statement.

THE RIGHT TO ERASURE (TO BE FORGOTTEN)	Individuals have the right to have their data 'erased' in certain circumstances. An individual may have the right to obtain from an organisation the erasure of personal data where: ▪ personal data are no longer necessary for the purpose(s) for which they were collected or processed; ▪ the personal data are processed unlawfully, that is, in some way which is in breach of the Acts; ▪ the personal data have to be erased with a legal obligation An individual also has a right to erasure of their personal data where: ▪ the individual withdraws consent to processing and there is no other legal reason for processing; ▪ the processing is based on legitimate interest and the individual objects and the company cannot demonstrate that there are overriding legitimate grounds for the processing.
THE RIGHT TO RESTRICT PROCESSING	A restriction on processing means that the organisation may only store the data; it may not further process the data. Individuals have the right to have the processing of their personal data restricted in certain circumstances. For example: ▪ If an individual lodges a concern with the organisation that the personal data held by that organisation is inaccurate or that legitimate interest which the organisation relies upon to process does not exist, the organisation may restrict the processing of that individual's personal data for the period while the organisation is investigating the individual's concern. ▪ The processing is unlawful but the individual objects to erasure and requests restriction instead; ▪ The organisation has no further need for the data but the individual requires the organisation to retain the personal data establish, exercise, or defend legal claims.
THE RIGHT TO OBJECT TO PROCESSING	An individual has a right to object to the processing of their personal data. This is a limited right. It applies where the organisation relies on legitimate interests grounds as a legal basis for the processing of personal data. In such circumstances, an individual may object to the company processing his/her personal data. On receipt of the individual's objection, the organisation must cease processing of the individual's personal data unless: ▪ The organisation can demonstrate compelling legitimate grounds which override the interests of the data subject; or ▪ The processing of the data is necessary for the establishment, exercise or defence of legal claims.
THE RIGHT TO DATA PORTABILITY	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability applies in limited circumstances, that is, where: ▪ the individual has provided the personal data to the company; ▪ the processing of the personal data is based on the individual's consent or for the performance of a contract; and ▪ the processing is carried out by automated means. This means that the right does not apply to paper records.
THE RIGHT TO NOT BE EVALUATED ON THE BASIS OF AUTOMATED PROCESSING, INCLUDING PROFILING	The GDPR include restrictions on decisions based solely on automated processing, which could include profiling. Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

8. ENHANCED RULES FOR TRANSFERS OF DATA OUT OF THE EU

The GDPR does not change the rules relating to cross-border transfers too significantly, and in many respects it enhances and improves the mechanisms that are currently permitted. It also introduces some new transfer mechanisms.

The GDPR retains the general prohibition on transferring personal information out of the EU, unless the destination jurisdiction/ international organisation has been deemed "adequate" by the EU Commission or a permitted transfer mechanism (as set out in the GDPR) is in place. The criteria by which the EU Commission can deem a country, territory or international organisation as "adequate" have been tightened, and adequacy decisions will not be open-ended – they remain valid under the GDPR only for a maximum period of 4 years, and then must be re-examined.

In terms of new mechanisms:

- ***Agreements between public bodies:*** Cross-border transfers can take place between a public authority in the EU and a public authority in a third country, on the basis of agreements between those public authorities and whereby those public authorities ensure compliance with the GDPR. These transfers do not require prior approval of a data protection supervisory authority.
- ***Administrative arrangements between public bodies:*** Likewise, cross-border transfers can take place under administrative arrangements between EU- and third country public authorities (for example, based on a Memorandum of Understanding between them), as long as those arrangements contain adequate protections for the individuals whose data are affected. However, unlike agreements between public authorities, these administrative arrangements will require prior approval of the relevant data protection supervisory authority.
- ***Binding Corporate Rules:*** Binding Corporate Rules ("BCRs") are now formally recognised by the GDPR, subject to approval by a data protection supervisory authority. (They were not specifically listed as a permitted transfer mechanism in the Data Protection Directive; rather, they were based on various Article 29 Working Party papers and from data protection supervisory authority guidance.) The GDPR sets out the criteria to be met if BCRs are to be approved by EU data protection supervisory authorities. This includes that the BCRs must contain a mechanism to make them legally binding on all member companies of the relevant corporate group; that the BCRs must specify the purposes of the transfer and the categories of data affected by the transfer; they must reflect the requirements of the GDPR; they must confirm that the EU-based data exporters within the group accept liability on behalf of the entire group for any unlawful processing; outline and explain complaint procedures and provide for compliance mechanisms by the members of the corporate group. Once the BCRs meet the relevant criteria, the examining data protection supervisory authority must approve them.
- ***DPC-Approved Data Transfer Clauses:*** Apart from the Standard Contractual Clauses (SCCs) that are approved by the EU Commission, individual member state data protection supervisory authorities are given the power to adopt their own model transfer clauses. These clauses can be incorporated into a wider contract, and will not require further approval for use as long as they are not amended. Ad-hoc negotiated contractual clauses can also be used as valid transfer mechanisms, but subject to case-by-case approval by the relevant data protection supervisory authority.
- ***Codes of Conduct:*** Cross-border transfers can take place on the basis of an approved code of conduct which governs specific categories of data controllers and/or processors. The adoption of codes of conduct related to data processing is dealt with in a fairly detailed way under Articles 40 and 41 GDPR, including by specifying the issues they need to deal with, how they are to be binding on the members of the relevant group, and how their use is to be monitored. Article 40(5) GDPR provides a mechanism for approval of the drafted code by data protection supervisory authorities. Once approved, the European Data Protection Supervisory Board must make them publicly available. If the approved code covers cross-border data transfers, and there are binding and enforceable commitments to safeguard the data placed upon the proposed recipient of the data in the third country, then the code can be used as a permitted transfer mechanism by the adherents to the code.
- ***Certification:*** In a similar way to codes of conduct, the GDPR makes provision and establishes mechanisms for organisations' processing activities to be formally certified as GDPR-compliant, for periods of up to three years at a time. Again, if the organisation benefits from an approved certification, and there are binding and enforceable commitments to safeguard the data placed upon the proposed recipient of the data in the third country, then the certification can be used as a permitted transfer mechanism by the certified organisation.

The existing mechanisms (such as individual consent; fulfilling a contract with the individual; establishment, exercise or defence of legal claims; and protecting the individual's vital interests) are all retained, albeit that some of the obligations have been tightened up. For example, in relation to consent, the individual must provide explicit consent (where previously, the consent could be "unambiguous") and they must have been informed of the possible risks arising from any data transfer in advance.

9. ONE-STOP SHOP FOR DATA PROTECTION REGULATION

One of the frustrations of the current EU data protection regime for organisations operating across a number of EU member states is that it is sometimes uncertain which data protection supervisory authorities regulate them. The GDPR recognises this, and it introduces a "One-Stop-Shop" mechanism of regulation. What this means is that if an organisation has establishments in a number of member states, the data protection supervisory authority in its "main establishment" will regulate its data processing activities across the EU. Where other data protection supervisory authorities seek to regulate the organisation in respect of data processing taking place in their territory, the "lead authority" can take over that investigation or action. This One-Stop-Shop mechanism is welcome, in that it should lead to greater consistency of regulation of organisations, and provide them with greater certainty.

The One-Stop-Shop mechanism has been one of the early subjects of GDPR-related guidance from the Article 29 Working Party, in December 2016. In particular, the guidance gave some useful insight into how regulators will assess the place of main establishment of an organisation operating across the EU. The main establishment will usually be the place of central administration of the organisation, for example its designated EU HQ. However, the key issues will be:-

- Where are the decisions taken about the purposes and means of the processing?
- What entity has the power to implement decisions concerning the processing activity?

Other factors will include the location of directors with overall management responsibility for the cross-border processing activities. One interesting issue raised by the guidance is that regulators consider that different processing activities can have different "main establishments". For example, in relation to a large banking and finance organisation, the bank might have its HQ in Frankfurt (and so its main establishment insofar as data processing relating to banking will be Frankfurt); however, its insurance department may be located in Vienna (whereupon its main establishment for insurance-related processing will be Vienna).

What to do and how to prepare

Organisations that operate across a number of EU member states will need to consider whether they need to or should make any changes to their operational structures in order to provide themselves with more certainty about who regulates them and where.

10. DATA PROTECTION BY DESIGN AND DATA PROTECTION BY DEFAULT, AND THE OBLIGATION TO CONDUCT DATA PROTECTION IMPACT ASSESSMENTS

DATA PROTECTION BY DESIGN AND DATA PROTECTION BY DEFAULT

The GDPR specifically recognises two principles "data protection by design" and "data protection by default". These principles place an ongoing obligation on organisations to ensure that all processing of personal data throughout the organisation protects the privacy rights of individuals.

Essentially, the principles require that an organisation's entire practices and policies are automatically privacy friendly. The GDPR requires the data controller to adopt internal policies and implement measures which comply with principles "data protection by design" and "data protection by default". The GDPR suggests that data controllers take the following measures:

- Minimise the processing of personal data
- Pseudonymise personal data as soon as possible
- Have complete transparency with regard to the functions and processing of personal data
- Enable the data subject to monitor data processing

The GDPR requires that in the design and creation of new products or services the data protection and privacy rights of individuals are considered throughout the design stage. Similarly, the principles of data protection by design and default should also be taken into consideration in the context of public tenders.

The GDPR includes a certification procedure whereby an organisation may obtain a recognised data protection certification. If an organisation successfully obtains such a certificate, this may be used by a data controller to demonstrate compliance with the principles of data protection by design and data protection by default.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The GDPR specifically recognises two principles "data protection by design" and "data protection by default". These principles A DPIA is a process followed by an organisation which carefully and systematically considers the potential risks a proposed project might have on the privacy of individuals. The purpose of a DPIA is to identify all possible risks attached to the proposed project prior to the processing of personal data taking place. The GDPR places a mandatory obligation on data controllers to conduct a DPIA in certain situations. It is hoped that the positive impact of a DPIA is that the risk of potential personal data breaches is minimised as the organisation is in a position to address and mitigate any risks to personal data before the processing takes place.

When will a DPIA be necessary?

The GDPR requires data controllers to complete a DPIA prior to commencing a new processing activity (in particular where new technologies will be used) which is likely to result in a high degree of risk for data subjects. In particular, a DPIA will be necessary where:

- the processing involves a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person;
- special categories of personal data and personal data relating to criminal convictions and offences will be processed on a large scale; and
- the processing involves a systematic monitoring of a publicly accessible area on a large scale.

In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless. A DPIA is a useful tool to help data controllers comply with data protection law. This will also ensure compliance with the GDPR.

National supervisory authorities will be required to publish a list of the kind of processing activities which will require a DPIA. While the Irish DPC has not yet published such a list, the Article 29 Working Party has outlined some examples of processing that will require a DPIA, for example:

- a hospital processing its patients' genetic and health data;
- the use of a camera system to monitor driving behaviour on highways where the technology will include an intelligent video analysis system which can single out cars and recognize number plates;
- a company monitoring its employees' activities, including monitoring the employees' work station, internet activity, etc.
- Similarly, the Article 29 Working Party has suggested some examples of processing that will not require a DPIA, for example:
- an online magazine using a mailing list to send a generic daily digest to its subscribers;
- an e-commerce website displaying adverts for vintage car parts involving limited profiling based on past purchases behaviour on certain parts of its website.

It should also be noted that while the obligations under the GDPR apply to processing operations initiated after the GDPR becomes applicable on 25 May 2018, the Article 28 Working Party strongly recommends that data controllers conduct DPIAs for processing operations already underway prior to May 2018.

At this stage, we recommend that organisations should now start to assess whether current and future projects will require a DPIA.

How should a DPIA be conducted?

A DPIA may concern a single processing operation or cover multiple processing operations that present similar risks.

While the controller is responsible for ensuring a DPIA is completed, the controller may appoint someone else within or outside the organisation to complete the DPIA. If the controller has appointed a DPO (as discussed above), the controller must seek the advice of the DPO when conducting the DPIA.

The GDPR recognises that a DPIA can involve discussions with relevant parties/stakeholders and provides that where appropriate, a controller must seek the views of data subjects (or their representatives) on the intended processing.

The GDPR sets out the minimum issues that a DPIA must consider, namely:

- the envisaged processing operations and the purposes of the processing
- an assessment of the necessity and proportionality of the processing
- an assessment of the risk to the rights and freedoms of the data subjects
- the measures envisaged to address risks and demonstrate compliance with the GDPR.

It is crucial that the data controller maintains clear records throughout the DPIA process to demonstrate that these issues were carefully considered in the course of the DPIA.

In guidance relating to the GDPR, the Irish DPC notes that where the DPIA indicates that the risks identified in relation to the processing of personal data cannot be fully mitigated, data controllers will be required to consult the DPC before engaging in the proposed processing.

What to do and how to prepare

Organisations will need to consider their planned projects and data processing activities, with a view to considering whether they need to conduct a DPIA in order to underpin them.

DAMIEN YOUNG
PARTNER
dyoung@philiplee.ie
@philipleelaw

ANN HENRY
PARTNER
ahenry@philiplee.ie
@AnnHenryIP

ANNE BATEMAN
PARTNER
abateman@philiplee.ie
@philipleelaw