THE
NATIONAL LAW REVIEW

# EU's New Data Protection Regulation – Are Your Cybersecurity and Data Protection Measures up to Scratch?


Article By
Tax Practice at Cadwalader
Cadwalader, Wickersham & Taft LLP
Clients & Friends Memos

- Communications, Media & Internet
- Global
- European Union

Monday, March 6, 2017

In the context of increasing cyber-attacks on major corporate organisations, small businesses and government, data protection and cybersecurity is a hot topic. Added to this, the GDPR—a strict new regulatory regime in Europe—will commence in May 2018 and has implications for both non-European and European-based organisations.

Organisations which come within the scope of the GDPR, including organisations located outside of the EU, will be required to comply with more stringent data protection compliance obligations and face the prospect of exposure to multimillion-dollar fines and class actions if they breach these obligations. It is, therefore, crucial for non-EU established companies carrying out activities that fall within the GDPR to develop an understanding of their obligations under the GDPR, and take steps to ensure that they will be able to comply with their obligations when the GDPR starts to apply next year.

This Memo provides an overview of the GDPR and its implications for your business, whether based in the EU, the United States, or further afield and addresses the following key issues:

## I. Introduction to the GDPR?

The GDPR is an EU Regulation aimed creating a uniform set of data protection rules across Europe which reflect the realities of the digital age. The GDPR entered into force on 24 May 2016 but does not apply until 6 May 2018; this will give organisations an opportunity to prepare to meet the new obligations that the GDPR imposes. The GDPR will replace the previous General Data Protection Directive[1] (the "**Directive**"), which was implemented in the UK by the Data Protection Act. Because the GDPR is an EU Regulation (as opposed to a Directive[2]), it will apply directly in all EU Member States[3] (including, for now, the United Kingdom[4]) without the need for each Member State to pass its own legislation implementing the GDPR. This is good news because it likely will lead to greater consistency in the application of the GDPR throughout the EU compared with the current Directive. However, the GDPR contains various provisions still enabling Member States to legislate on certain data protection matters, which could result in some divergent approaches in different Member States.

The GDPR's material scope is very broad. It applies to the "processing" of personal data by automated means or as part of a filing system and, so, typically will capture all personal data that is collected and entered into an organization's computer or filing systems in the course of an organization's activities (for example, a bank that enters a customer's personal data into its computer system to open a bank account would be "processing" that customer's personal data). The GDPR does not cover processing of personal data by authorities in relation to the prevention, detection and investigation of crime, and people processing data for personal or household activities are also not in scope.

The GDPR imposes wide-ranging obligations on businesses, which include:

- adopting mandatory data protection principles for organisations;
- creating individual rights in relation to personal data, including rights of access and rights to have personal data destroyed;
- imposing obligations relating to data governance, security of processing, and reporting of personal data breaches;
- restricting the transfer of personal data outside of the EU unless certain criteria are met; and
- setting forth potential remedies, liabilities and administrative fines for non-compliance.

The territorial scope of the GDPR is broader than current data protection laws. EU-based companies that control or process data always have needed to comply with EU data protection laws (whether or not the personal data was processed in the EU). However, the GDPR also applies to "controllers" or "processors"[5] who are not established in the EU but are processing the personal data of people who are in the EU, if the processing activities relate to:

- the offering of goods or services to data subjects in the EU (regardless of whether payment is required)[6]; or

- the monitoring of a data subject's behavior, where that behavior takes place in the EU. Monitoring includes the tracking of individuals online in order to create profiles (e.g., to enable the provision of customized recommendations).

## II. Data Protection Principles

Underlying the GDPR are six principles relating to the processing of personal data (the "**Data Protection Principles**"). These are set out in Article 5, and provide that personal data should be:

- processed lawfully, fairly and transparently;
- collected and processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purpose for which it is processed;
- accurate and up to date;
- kept in a form permitting identification of data subjects for only as much time as necessary; and
- processed securely (including protections against processing data without a data subject's consent, unlawful processing,[7] accidental loss and destruction or damage) whilst using appropriate technical or organisational measures.

## III. Data Controllers and Processors

Like the Directive, the distinction between data "controller" and data "processor" is central to the GDPR because the characterisation as either controller or processor or both governs the extent of an organisation's obligations under the GDPR. The definition of controller and processor are broadly the same as under the Directive. This means that if under the Directive an organisation is designated a controller and/or a processor, such designation is unlikely to change under the GDPR:

- A **controller** is defined as any individual or organisation, including public authorities, agencies or other body, which, on its own or together with others, "determines the purposes and means of processing of personal data." Essentially, the controller determines how and why personal data is processed.
- A **processor** is defined as any individual or organization, including public authorities, agencies or other body, which processes personal data on behalf of the controller.[8]

The European Commission ("**EC**") Article 29 Working Party ("**WP29**") provided guidance on the definitions of controller and processor under the Directive by reference to various practical examples. One of these examples was a financial institution using an outsourced call centre. The WP29 stated that such a financial institution would be a data controller because it determines what information the call centre receives and how the call centre may use it. The call centre, which acts on instruction of the financial institution in terms of the data it collects and

transmits to the financial institution, would be the processor in this situation. By way of another example, the WP29 referred to social network service providers who provide online communication platforms which allow individuals to publish and exchange information with others. The WP29 stated that social networks of this sort are data controllers because they determine the purpose and the means of the processing of the data contained in the information published and exchanged by individuals.

Many organisations will be both a data controller and processor sometimes for the purpose of the same personal data or for the purposes of different personal data. For example, a sub-contractor who contracts to undertake certain processing activities on behalf of a controller is likely to have its own responsibilities as a controller with respect to personal data it holds about its own employees, clients or sub-contractors, distinct from any responsibility to process data on behalf of the controller client. For example, a call centre which contracts to undertake the role of telephone information service for customers of a bank will be a processor for the purpose of personal data it processes on behalf of thel bank – e.g. customer personal identification information and account information. It will also be a controller with respect to information it holds about its own employees. The call-centre may also sub-contract the processing of its employee information to a HR firm, in which case the HR firm would be a processor of the call centre's employee personal data. It is critical therefore for organisations to carefully consider when it may be acting as a controller.

***Tip!*** *If in doubt as to whether your organisation is a controller or a processor (or both), it is very important that you seek appropriate advice to enable your organisation to meet its respective obligations under the GDPR.*

Controllers are responsible for ensuring compliance with the Data Protection Principles. Controllers' obligations include implementing appropriate technical and organisational measures which ensure and demonstrate that processing activities are GDPR-compliant. These measures include implementing an appropriate data protection policy and ensuring that the Data Protection Principles and appropriate safeguards are addressed and implemented in both the planning and implementation phases of new services or processing measures. Further specific obligations on controllers are discussed in the sections below.

A controller may appoint only a processor who guarantees compliance with the GDPR. The processor must be appointed by a binding written agreement containing certain minimum standards as prescribed by the GDPR, which include, for example, that the processor will act in compliance with the controller's instructions contained in the contract and guarantee the security of personal data it processes.

Processors have specific legal obligations placed on them by Articles 28-37 of the GDPR. These include:

- maintaining records of personal data and processing activities, including details of all controllers for which it operates, details of any co-processors, details of the appointed data protection officers ("**DPOs**"), the categories of processing undertaken, technical and organisational security measures in place and details of third-country data transfers;[9]

- executing a binding contract with the controller prior to processing any data on behalf of the controller;[10]
- processing personal data only in accordance with the controller's instructions;[11] and
- informing the controller if it believes an instruction to provide information to the controller breaches the GDPR or any other EU or Member State law.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR, in fact, places further obligations on you to ensure your contracts with processors comply with the GDPR.

***Tip!*** *Organisations which act or intend to act as controllers and/or processors should commence a GDPR compliance review of their supply contracts, ensuring that the purpose, nature and length of the processing to be undertaken by the processor on behalf of the controller is identified clearly.*

## IV. Data Protection Officers

Controllers and processors have an obligation to designate a DPO[12] if one of the following descriptions applies:

- the organisation's processing is carried out by a public authority or body;[13]
- the organisation's core activity(s) consists of processing operations, which requires regular and systematic monitoring of data subjects on a large scale; or
- the organisation's core activity(s) consists of monitoring individuals (systematically and on a large scale) or processing special categories of personal data on a large scale.

The European Commission Article 29 Working Party ("**WP29**") has clarified that, by "core activity," it means that processing is a primary activity that is necessary to the key operations in order to meet the organisation's goals, and, thus, is not an ancillary activity of the organisation.

Whether or not an organisation needs to appoint a DPO will not always be clear. The WP29 guidance on the DPO requirement provides that unless it is obvious that an organisation does not need a DPO, the organisation must produce a document containing internal analysis of why a DPO has or has not been appointed. This will serve to demonstrate whether or not organisations have evaluated appropriate relevant factors in making a decision to appoint or not appoint a DPO.

Article 39 of the GDPR requires that DPOs conduct at least the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other EU or Member State data protection provisions;
- to monitor compliance with the GDPR, with other EU or Member State data

protection provisions and with the policies of the controller or processor in relation to the protection of personal data (including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits);

- to provide advice where requested as regards the data protection impact assessment and monitor its performance;

- to cooperate with the supervisory authority and to be the contact point for the supervisory authority on issues relating to processing, including the prior consultation.

In undertaking its duties, the DPO must have "*due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.*"[14]

The WP29 has issued guidance on DPOs and has noted that while DPOs do not require a minimum level of expertise, "*it must be commensurate with the sensitivity, complexity and amount of data an organisation processes.*"[15] This means that where particularly sensitive data is being processed, or involves particularly complex processing methods, the DPO is likely to need a higher level of qualification and support. The WP29 has stated that the individual(s) appointed to the role of DPO should be carefully chosen and regard taken to the kinds of data protection issues likely to arise in the appointing organisation.

***Tip!*** *If in doubt, seek advice as to whether your organisation must designate a DPO. Clearly document and explain the DPO's role and responsibilities and ensure that the DPO understands these.*

## V. Consent and Justification for the Processing of Personal Data

Similar to the Directive, consent will mean a lawful basis to process personal data under the GDPR. However, under the GDPR there will be stricter conditions for obtaining consent to process personal data, and controllers must be able to demonstrate consent. The conditions are that:

- the data subject must have the right to withdraw consent at any time;

- there is a presumption that consent will not be valid unless separate consents are obtained for different processing activities, and there is a presumption that bundling consent mechanisms with other consent clauses is not permitted; and

- the implicit "opt-out" consents which are permitted under the Directive have to be replaced with explicit statements of affirmative consent.

***Tip!*** *Use the lead time to the implementation of the GDPR to evaluate your current consent clauses and determine whether and how you will need to amend such clauses to comply with the stricter requirements which will come into effect in May 2018.*

## VI. Special Categories of Data

The GDPR maintains the Directive's distinction with respect to the requirements for processing "special categories of personal data" ("**special data**") distinct from personal data. It also expands the range of data which constitutes special categories.[16] Special data (which in the UK is known as "sensitive data") will expressly include "genetic data" and "biometric data" if it is processed in a way that uniquely identifies a person.

Under the GDPR, data controllers must show that they have a legal basis to process special data. In addition, the GDPR creates a new requirement that requires controllers to undertake a Privacy Impact Assessment ("**PIA**") in circumstances where processing will likely result in a high risk to the rights and freedoms of data subjects.[17] For any large-scale processing of special categories of data, PIAs will be necessary. If the PIA indicates that the processing will likely result in a high risk to individuals in the absence of the data controller adopting measures which will mitigate such risk, then the data controller must consult with the relevant Supervisory Authority ("**Authority**") prior to processing the special data.

***Tip!*** *Ensure that policies and procedures provide for a timely assessment of whether a PIA is before any special category of data requires is processed. Consider ensuring that controller-processor contracts include measures for PIAs to be undertaken prior to the processing of any special category data.*

## VII. Security Measures

The GDPR requires controllers and processors to implement appropriate technical and organisational measures to guarantee a level of security appropriate to the risk.[18] The appropriateness of security measures will be measured against the context and purposes of the processing as well as the risk and severity to the rights and freedoms of data subjects.

The kinds of factors which may be analysed to determine the appropriateness of the measure include: whether the data is of a particularly sensitive nature; the risks to data subjects in the event of a breach; and the relative costs involved in implementing certain types of security measures.

The GDPR provides that the following measures may be appropriate:

- encryption;
- pseudonymisation;
- measures which ensure the confidentiality, integrity and resilience of processing systems and services;
- methods which enable the timely access, restoration or availability to personal data in the event of an incident; and
- regular tests and evaluation to ensure that the measures implemented meet their desired objective of maintaining security of data processing.

***Tip!*** *This is a good opportunity for you to review your organisation's cybersecurity*

*measures to ensure that they are adequate to meet current cybersecurity threats.*

## VIII. Reporting Breaches

Controllers must report any breach of personal data to the competent Authority (in the UK this means the Information Commissioner's Office)[19] without undue delay and where feasible within 72 hours after becoming aware of the breach, unless it is considered unlikely to result in a risk to the rights and freedoms of data subjects.[20] Controllers are required to explain to the Authority the reasons why any notification occurred after the 72-hour period.

Failure to comply with breach reporting requirements under the GDPR will not just result in regulatory scrutiny, negative PR and potential loss of business; there are also very real financial penalties which the regulators have in their armories for serious failures: up to the higher of 2% of annual global turnover or 10 million Euros (approximately USD105 million).

## IX. Communication of a Personal Data Breach to the Data Subject

Where the result of a personal data breach likely will lead to a high risk of impact to the rights and freedoms of a data subject, without undue delay, the controller also is obliged to inform the data subject of the breach.[21] The communication must use clear and plain language to explain the nature of the breach and contain not less than the following:

- the name and contact details of the relevant DPO, and/or any other relevant contact person;
- the likely impacts of the data breach; and
- the measures taken or proposed to be taken by the data controller to deal with the breach and/or mitigate its consequences.

However, controllers are not required to communicate the breach to the data subject where one more of the following conditions has been met:

- technical and organisational measures, such as encryption, were applied to the personal data such that it would be unintelligible to any person not authorized to access the data;
- the controller has taken steps to ensure that the originally high risk is no longer likely to materialize; or
- where making an individual announcement to each data subject would be a disproportionate response compared to efficacy of making a public announcement.

Where a breach is reported to an Authority and not to the data subjects, the Authority may require the controller to notify affected data subjects.

Processors are required to notify controllers of a personal data breach without undue delay.[22] Particularly troubling for businesses seeking to comply with the GDPR's notice provisions is that the GDPR does not provide definitions of critical concepts like "breach" or "high risk of impact" leaving businesses in the dark as to just what types of breaches – or potential breaches – must be reported to regulators and customers. For example, if an organization merely suspects that a breach has occurred and cannot determine, for certain, whether any customer data was stolen, does the organization then have an obligation to report the possible breach to the relevant authority or customers?

***Tip!*** *In the absence of further guidance, the best practice for organisations is, from the outset, to minimise breaches by developing, implementing and constantly monitoring the efficacy of policies designed to assist staff to identify risks and demonstrate that that the right precautions were put in place to prevent the breach. Organisations should develop an 'action plan' to assist staff with knowing how to deal with an actual or suspected breach (including meeting reporting obligations within the 72-hour deadline) in compliance with the GDPR.*

## X. Data Subject Rights to Compensation

Individuals affected by a breach of their rights may claim compensation for material or non-material damage (such as distress), a position that already applies under UK case law, where in the past individual data subjects in the most extreme data protection breach cases have been awarded up to £260,000 (approximately USD 318,890)[23] in compensation. Whereas previously only the data controller could be subject to a claim for compensation, a claim now may be brought against both the controller and the processor. The GDPR also enables group claims to be brought—although, unlike in the US, the ability to bring a group claim is limited to representative not-for-profit bodies, such as a consumer protection body, mandated by a data subject—increasing the potential value of claims for compensation that companies may face in the event of a data breach.

***Tip!*** *Contracts between controllers and processors should address allocation of liability in the event of a data breach.*

## XI. Powers of Supervisory Authorities to Impose Fines and Penalties

The respective Authority in each member state will, with various corrective powers, include the power to:

- issue warnings and reprimands to controllers and processors that have or are likely to infringe the GDPR;
- order compliance with a data subject's requests to exercise rights set out in the GDPR;
- order a controller or processor to bring processing operations into compliance with the GDPR (including specifying how and when by);

- impose temporary or permanent limits on a controller's or processor's actions, including banning processing of personal data;
- order rectification, erasure, or restriction of processing of personal data;
- impose administrative fines of up to the higher of 4% of worldwide annual turnover or €20 million Euros (USD 21 million) in the preceding financial year; and
- prohibit the transfer of information to a recipient in a third country.

These powers are wide-ranging, and the size of potential fines is significantly increased from the position under current data protection rules.

The current maximum fine that can be imposed in the UK is £500,000 (approximately USD 613,000). The highest fine that actually has been imposed in the UK was the £400,000 (approximately USD 490,000) fine imposed on a telecoms company, TalkTalk, following a data breach which resulted in 156,000 customers having their personal data stolen and 15,000 customers having their bank account details stolen.

This significant increase in the maximum possible fine means that an organisation's potential risk exposure for breaches of data protection obligations will increase by a considerable magnitude. The potential liability that organisations are exposed to means that we expect data protection obligations to gain considerable prominence in internal risk-management discussions.

## XII. Transferring Data outside the EEA[24]

Like the Directive, the GDPR imposes significant obligations on those wishing to transfer data outside the EEA affecting multinational organisations that have operations inside and outside the EEA and organisations in the EEA that, for example, use international supply chains.

In respect of the transfer of data by processors in the EEA to recipients based in a non-EEA country, the GDPR's obligations are substantially the same as the Directive's. Processors may transfer data only to an individual or organisation based in a non-EEA country where:

- the EC has made an adequacy decision with respect to that third country or where the data will be received[25]; or
- absent an EC adequacy decision,[26] the controller or the processor has provided appropriate safeguards, and on condition that data subjects have enforceable rights in that country with respect to the data.
- Similar to the Directive, the following methods for the transfer of personal data will be recognised mechanisms providing for adequate safeguards under the GDPR:
- standard contractual clauses which are adopted and published by the EC or by an EC-approved supervisory authority;[27]

- binding corporate rules whereby the non-EEA receiver's rules require it to comply with certain minimum GDPR standards for the receipt and processing of personal data;
- legally binding and enforceable instruments between public authorities; and
- an approved binding and enforceable code of conduct, based on the Article 40 scheme, or an approved binding and enforceable certification mechanism based on the Article 42 scheme, each made by the controller or processor in the third country to apply the appropriate safeguards and, in particular, with respect to protecting the data subject's rights.

Under the GDPR it will be unlawful to transfer personal data outside the EEA because of a legal requirement of a third country, unless the requirement is based on an international agreement or another ground for which the transfer applies. In other words, unless an EU member state has expressly opted out of this provision, the GDPR may, in some circumstances, prohibit any organisation from complying with a demand by a regulator outside of the EU for production of EU customer data. The UK, however, has opted out of this provision.

## XIII. The EU-US Privacy Shield and the GDPR

On 12 July 2016 the EC adopted its Adequacy Decision, enabling companies to rely on the Privacy Shield. On 26 July 2016, only a few weeks after the Adequacy Decision, the WP29 stated that it did not consider that the Privacy Shield adequately addressed EU privacy requirements. In particular, the WP29 expressed its regret in respect of matters including:

- the lack of certainty as to how the Privacy Shield Principles apply to data processors;
- the absence of "concrete assurances" that bulk collection of personal data in the US will not occur again; and
- no specific rules on automated decisions and a general right to object.

Added to this, in October 2016, privacy advocacy group Digital Rights Ireland filed a claim in the General Court division of the Court of Justice of the EU (the "**CJEU**"), alleging that the Privacy Shield failed to guarantee an adequate level of data protection as required by EU law. This follows on from the October 2015 decision of the CJEU that the EU-US Safe Harbor mechanism was illegal because it was incompatible with the fundamental rights of EU citizens. It was this decision which led to the development and implementation of the EU-US Privacy Shield. The Safe Harbour case also was brought by Digital Rights Ireland.

The GDPR makes no reference to arrangements for the transfer of data from the UK to the US. Given the WP29's criticism of the Privacy Shield, EEA-based organisations should carefully monitor any guidance by the WP29 on the adequacy of the Privacy Shield or any additional necessary requirements to transfer data from the EEA to the US.

[1] Directive 94/46/EC.

[2] By contrast, a Directive is not effective without separate implementing legislation in each Member State.

[3] Note that it currently does not apply to the EEA (the European Economic Area, which consists of the EU plus Iceland, Lichtenstein and Norway) but it is in the process of being considered for adoption, and will likely be adopted by the EEA before the Regulation starts to apply.

[4] The UK is likely to remain part of the EU until at least 2019, after the GDPR has started to apply. All EU laws will continue to apply in the UK until the UK actually leaves the EU. The UK government also has announced its intention to pass a "Great Repeal Bill" which—contrary to what its name suggests—will ensure that, when the UK leaves the EU, all EU laws that are then in force will continue to apply. The GDPR, therefore, is going to be part of the legal landscape in the EU and the UK for the foreseeable future.

[5] These concepts are further defined below.

[6] This requires more than simply having a website that can be accessed from within the EU. There must be an intention to offer goods or services to data subjects in the EU. This could be evidenced by, for example, including on the website the possibility of using a language and currency of a Member State, or referring to customers or users in the EU.

[7] Examples of unlawful processing include processing that involves (i) a criminal offence, (ii) a breach of a duty of confidence (for example, if the personal data was collected in circumstances where confidentiality was expected), or (iii) a breach of an enforceable contractual obligation.

[8] It is also possible for one entity to be a co-controller or a co-processor with another entity.

[9] Such must be provided to the relevant regulator on request. A processor will be exempt from the requirement to maintain a record if it has less than 250 employees and, provided that the processing does risk the rights and freedoms of individuals, is not more than occasional and does not include special data (e.g., sensitive personal data).

[10] The GDPR controller—processor contractual requirements are set out in Article 28(3). The contract must cover the purpose, nature and length of the processing to be undertaken by the processor as well as establish the categories of data to be processed, the obligations and rights of the controller. Article 28(8) permits each member state's Supervisory Authority to adopt standard contractual clauses which controllers and processors may incorporate into their respective contracts. Clients should keep a close eye on the publication of such standard contractual clauses by Supervisory Authorities.

[11] Therefore, it will be important for controllers and processors to contract clearly with respect to the scope of the processor's activities.

[12] GDPR, Article 37(1).

[13] The GDPR does not define what constitutes a ”public authority or body.” The Article 29 Working Party, an EU advisory body consisting of a representative of each Member State’s data protection authority, considers that such a notion is to be determined under national law.

[14] e GDPR, Article 39.

[15] *See* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

[16] GDPR, Article 9.2.

[17] GDPR, Article 35.

[18] GDPR, Article 32.

[19] Further discussion on the role of the competent Authority is discussed below at item VII.

[20] GDPR, Article 33.

[21] GDPR, Article 34.

[22] GDPR, Article 33.

[23] *Gulati & Ors v MGN Ltd* [2015] EWHC 1482 (Ch) – a case arising out of the notorious phone hacking carried out by Mirror Group Newspapers.

[24] It is assumed that the EEA will adopt the GDPR prior to May 2018, meaning that a ”third country,” for the purposes of the GDPR, will be a non-EEA country.

[25] GDPR, Article 45.

[26] GDPR, Article 46

[27] Such clauses operate in contracts between the EC transmitter of the data to the non-EEA receiver whereby the non-EEA receiver contracts to comply with certain non-EEA receiver contracts to comply with standards not less stringent than the GDPR requirements for the receipt and processing of standards and for the receipt and processing of data from the EEA.