The EU General Data Protection Regulation: The new data protection landscape

Rhys Hadden, Guildhall Chambers

Introduction

1. After a lengthy trilogue spanning nearly four years between the European Parliament, the European Commission and the Council of Ministers, the new EU data protection framework, the General Data Protection Regulation ("GDPR") was finally agreed at the end of 2015 and formally adopted in April 2016.

2. The GDPR aims to create stronger data protection laws within the UK and Europe, with the intention of making the region the safest in terms of data protection worldwide. All organisations that process the personally identifiable information of EU residents will be required to abide by a number of provisions or face significant penalties.

3. The GDPR will supersede national laws such as the UK DPA, unifying and harmonising data protection and easing the flow of personal data across the 28 EU member states. As a regulation (as opposed to another directive) the GDPR will be a single piece of legislation directly applicable across all EU member states without the need for implementing national legislation.

4. The GDPR requires all public and private sector organisations that hold European data to comply by 25 May 2018. It contains some onerous obligations, meaning it will have an immediate impact. This seminar will look at some of the key provisions and changes implemented by the GDPR and the potential impact these may have on businesses and the public sector in the UK.

The current regime

5. The current legal framework in the European Union relating to the protection of personal data mainly results from Directive 95/46/CE ("the 1995 Directive"), which set a minimum level of protection for the processing of data relating to individuals. In the UK, the 1995 Directive was implemented by the Data Protection Act 1998 ("DPA 1998").

6. The harmonisation step of 1995 came in the form of a EU directive. Following its implementation under national law member states eventually produced a patchwork of very different regulations. As a result, it is currently complex for businesses established

in several countries within the EU to roll out personal data processing on their various sites.

7. Furthermore, since 1995 technology has evolved significantly, particularly in the field of IT, telecommunications and the internet. The advent of the digital age has led to a radical shift in the volume, variety and the speed data is being produced. There is now ubiquitous use of social media and heavy reliance on cloud computing by individuals and businesses. Big data promises to deliver significant value, especially concerning analytics based on personal data. As a result of such a major shift in the uses of networks and data, revision of the framework set by the 1995 Directive became inevitable.

Implementation of GDPR

8. On 4 May 2016, the official texts of the GDPR and the new Directive were published in the EU Official Journal in all the official languages. The GDPR will enter into force on 24 May 2016 and shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU member states have to transpose it into their national law by 6 May 2018.

Key changes introduced by the GDPR

Expanded Territorial Scope

9. The GDPR has introduced 'European rules on European soil' by recasting the territorial scope of European data protection laws. Businesses, even if they are not 'established' in the EU, will be subject to the GDPR, if they offer goods and/or services to EU data subjects or they monitor behaviour of EU data subjects. As such, many businesses will need to appoint a representative in the EU. The Recitals to the GDPR offer some guidance about when a business may be subject to its reach. For example:

    - "offering goods or services"[1] suggests more than mere access to a website or email address but might be shown by use of a language or currency generally used in one or more of the member states with the possibility of ordering goods or services there and/or monitoring customers or users who are in the EU;

[1] Recital 23, GDPR

- "Monitoring of behaviour"[2] will occur where individuals are tracked on the internet by techniques which apply a profile to enable decisions to be made to predict personal preferences, behaviours and attitudes;

Data Protection Principles

10. The data protection principles, as set out in the DPA 1998, remain but they have been condensed into six as opposed to eight principles. Article 5 of the GDPR states that personal data must be:

    (a) Processed fairly, lawfully and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

    (b) Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes ('purpose limitation');

    (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed ('data minimisation');

    (d) Accurate and, where necessary, kept up to date ('accuracy');

    (e) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; ('storage limitation')

    (f) Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');

Changes to the definition of "personal data" and sensitive data

11. Article 4(1) GDPR defines personal data as follows: *'…any information relating to an identified or identifiable natural person … in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or*

[2] Recital 24, GDPR

social identity of that natural person'. This will usually include personal data that has been encrypted and online identifiers such as IP addresses.

12. The wider definition under the GDPR are likely to affect most processing acts of public sector authorities particularly as much peripheral information collected by them and 'relating to an individual' will now be caught within the new wider definition of 'personal data'.

13. Stricter rules also now apply to processing of special categories of personal data (sensitive data) such as medical information. What constitutes sensitive data has been widened and will now include genetic data, biometric data (e.g. retinal scans and fingerprints) and data concerning health[3].

Consent

14. Until now, consent has often been the default option when businesses and organisations seek to identify an applicable legal basis for their data processing activities. Consent is assumed to be easy, and organisations routinely rely on vaguely drafted, generic consent language, often used in circumstances in which individuals have no real choice.

15. The GDPR has significantly strengthened the criteria for consent. A data subject's consent to processing of their personal data must be 'freely given, specific, informed and unambiguous indication of the data subject's wishes' shown either by 'a statement or a clear affirmative action' which signifies agreement to the processing of personal data[4]. Recital 25 of the GDPR adds additional clarification, noting that mere silence, the use of pre-ticked boxes, or inactivity are unlikely to amount to consent. As before, consent to process sensitive personal data must be explicit[5].

16. A new provision underscores the fact that consent may be transient. Art.7(3) GDPR states that consent may be withdrawn at any time and stipulates that it must be as easy for an individual to withdraw consent as to give it. In considering whether consent has been freely given, account will be taken of whether the performance of a contract or service is made conditional on consent being given to process data that are not necessary for the performance of the contract. Attempts to bundle wide-ranging or generic consents into contractual language will no longer be permitted.

[3]Art. 9(1), GDPR
[4] Recitals 11 and 32, GDPR
[5] Art. 9(2)(a), GDPR

17. In addition to a formal definition, several additional 'conditions for consent' are set out in Art.7 of the GDPR. These represent a significant tightening up of the current requirements for establishing consent in the UK.

18. A data controller must be able to demonstrate that consent was given. Any new uses of data will require additional consents for those additional purposes. Art. 7(1) places an evidential burden on the data controller to demonstrate that consent has been obtained when it is relied on to process personal data. Furthermore, it is clear that any consent must be specific, and that the generic forms of consent that are often collected under the current regime will need to change. Controllers will no longer be able to embed consent clauses in lengthy terms and conditions but will need to present consent options in a manner clearly distinguishable from other matters, using clear and plain language[6].

19. Businesses and public bodies must begin the process of deleting information not collected by them but shared with them and/or seek active consent to use personal data they hold but did not create. As many public sector bodies also collect and process 'sensitive' data, a requirement for something much more akin to explicit consent from data subjects will apply.

20. As the test for valid consent is whether consumers (or customers/service users in the public sector environment) understand what they are agreeing to and make a meaningful choice in respect of processing of their data, public sectors will have to improve communications and consent around data collection, processing, retention and maintenance of such consents. Any processor can be called upon to demonstrate that it has considered the impact and effect of its processes and that it has assisted data subjects to make informed choices about how their data is used. All of this is likely to mean public sector organisations must undertake risk assessments and naturally, data processing and process reviews.

Children

21. One topic of huge debate about the GDPR relates to parental consent being required for children. Where online services ('information society services')[7] are provided to a child and consent is relied on as the basis for the lawful processing of his or her data, consent must be given or authorised by a person with parental responsibility for the

[6] Art. 7(2), GDPR
[7] Please note that the GDPR does not alter national legislation for offline data processing relating to children's data.

child[8]. However, the consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child[9].

22. The GDPR does not prescribe the age at which a person is considered to be a child. Instead, it entitles member states to set the age threshold anywhere between 13 and 16 (with the default being 16). Lack of enforced harmonisation is likely to cause difficulties for businesses offering services to children across multiple EU jurisdictions; or it may lead to businesses simply defaulting to the strictest age requirement approach to the varying age thresholds.

23. Data controllers are also required to take 'reasonable steps' to verify that consent has been given by the parent or guardian, 'taking into consideration available technology'[10]. However, age verification tools can be difficult to deploy, and companies will need to give careful thought as to how they verify that a child's consent is authorised by a parent (or equivalent). The position will be more complex where member states adopt different age limits to define a 'child'.

24. Processing of data relating to children is noted to carry certain risks, and further restrictions may be imposed as a result of codes of conduct[11].

Data subject rights

25. Article 2 of the GDPR has widened the list of rights that a data subject can exercise. The subject access right, rectification and being able to object to direct marketing remain. The time limit for responding to a subject access request has been reduced to one month, instead of 40 days[12], although there are some possibilities to extend this.

26. There has been a desire to strengthen data subject rights within the GDPR. To this end, there are a number of new data subject rights that have been included, for example data portability[13] (the right to require their data to be provided in a commonly used electronic form). One particularly prominent change is the right to be forgotten.

Right to erasure/right to be forgotten

[8] Art. 8(1), GDPR
[9] Recital 38, GDPR
[10] Art. 8(2), GDPR
[11] Art. 40(2)(g), GDPR
[12] Art. 12(3), GDPR
[13] Art. 20, GDPR

27. In 2014 the CJEU held that Google had to remove links to content containing inaccurate or outdated personal data made the so-called 'right to be forgotten' (*Google Spain SL v Agencia Española de Protección de Datos* (C-131/12); [2014] QB 1022). It has been accepted that individuals have a right to request internet search engines to remove, from the list of results displayed following a search made on the basis of a person's name, links to web pages that are published by third parties and containing information relating to that person, where such processing of personal data is incompatible with the 1995 Directive.

28. The GDPR has sought to give the concept a statutory footing. Article 17 introduces a right to erasure ('right to be forgotten') that will allow individuals a qualified right to request that their data be erased, provided certain grounds apply. Examples include where the data are no longer necessary for the purpose for which they were collected or processed, or the individual withdraws consent and no other legal ground for processing applies. Where relevant, businesses will have an obligation to erase the relevant personal data it holds concerning that individual without undue delay. However, the further retention of such data will be lawful in some cases where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims.

29. These concepts are not particularly new, but the GDPR takes it one step further. Where a data controller has made the information *public* (e.g. by posting it online) it is obliged to take reasonable steps to inform third parties that the data subject has requested the erasure of any links to, or copies of, that data. However, the obligations are not absolute as there are exceptions related to freedom of expression. Arguments about exactly how (and if) the provisions apply are inevitable.

Data governance obligations

30. One significant change for data controllers is the removal of the requirement to notify or seek approval from the supervisory authority (the member state's data protection regulators, e.g. the ICO) in many circumstances. The aim appears to alleviate the associated administrative and financial burden on data controllers.

31. In its place, the GDPR now places onerous accountability obligations on data controllers to demonstrate compliance. Organisations can be called upon at any time to provide

proof of compliance and that relevant organisational structures are in place. This will include requiring them to:

- maintain detailed records of their processing activities[14];
- conduct a data protection impact assessment[15] where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals;
- include data protection controls at the design stage of new projects involving the processing of personal data and, by default, e.g. data minimisation[16];

"One Stop Shop", the European Data Protection Board and supervisory authorities

32. Under the GDPR, member states will continue to have their own independent supervisory authorities tasked with national policing, enforcement of and compliance with data protection laws. However, with harmonisation at the core of the reforms, the GDPR has introduced a new process referred to as the 'one stop shop'. This is intended to ensure that where a data controller or processor carries out processing activities across multiple EU territories, it remains accountable only to one 'lead' supervisory authority (i.e. the supervisory authority of the member state in which the controller or processor has its 'main establishment').

33. Whilst the lead supervisory authority takes a primary coordinating role on enforcement in relation to any particular controller or processor, the GDPR sets out a detailed process by which it is required to liaise and cooperate with other supervisory authorities that have a legitimate concern or interest in the particular circumstances. Where supervisory authorities are unable to agree on a particular enforcement action or decision, the GDPR provides a procedure by which they can refer matters to the new European Data Protection Board (EDPB) for a binding decision[17]. This 'one stop shop' concept is potentially a means to simplify compliance for businesses and to ensure consistency of application of the GDPR. However, the detailed processes risk being highly administrative and bureaucratic, and potentially a bottleneck for supervisory authorities.

[14] By Art. 30, GDPR the current system of notification under the DPA 1998 will be replaced by a requirement for data controllers to keep an internal record in relation to all personal data they process. The record must include, among other things, details of the purpose of processing personal data, recipients, transfers to third countries, time limits for erasure as well as a general description of the technical and organisational measures in place protecting the data.
[15] Art. 35, GDPR
[16] Art. 25, GDPR
[17] Arts. 68 to 76 are concerned with the EDPB. The EDPB's obligations will include, among others, issuing opinions and guidance, ensuring consistent application of the GDPR and reporting to the Commission.

Mandatory Notification of Data Breach

34. The GDPR contains an obligation on data controllers to notify supervisory authorities of personal data breaches. In some cases this extends to the data subjects as well. Article 4 defines a personal data breach as: *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*.

35. Data controllers must notify their relevant supervisory authority (in the UK, the ICO) of any personal data breaches without undue delay and within 72 hours of awareness of the breach occurring[18]. A reasoned justification must be provided if this timeframe is not met. The only exception is where the breach is not likely to result in a risk to the rights and freedoms of the affected individuals. If there are high risks to the rights and freedoms of an individual (e.g. fraud or identity theft), the data controller must also communicate the breach to the individuals themselves and this must be done without undue delay[19]. This is a significant shift from the current UK position that only requires organisations in certain sectors (e.g. telecoms providers) to notify data breaches.

36. Article 31(5) GDPR requires all personal data breaches, no matter how insignificant, to be documented by data controllers. This should include the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance. Some, if not all of it, will also be accessible via FOIA requests, as many local authorities have already found[20].

Obligations of Data Processors

37. Another key change in the GDPR is that data processors now have direct obligations. This will include implementing technical and organisational measures, notifying the controller without undue delay of data breaches and appointing a DPO, if required (see below). The DPA 1998 currently only regulates data controllers (except if a data processor was to engage in criminal activity). The GDPR seeks to impose certain direct legal obligations on data processors as well as data controllers too. For example, the processor will have a responsibility for implementing appropriate technical and organisational measures for the security of personal data during its processing activities.

[18] Art. 33, GDPR
[19] Art. 34, GDPR
[20] See e.g. https://www.itgovernance.co.uk/blog/local-authorities-suffer-four-data-breaches-every-day/

Data processors are exposed to potential fines and claims from data subjects for failure to comply with the GDPR.

Data Protection Officers

38. In certain circumstances, businesses are required to appoint a data protection officer ("DPO") to enable those businesses to comply with its accountability obligations under the GDPR. This is a designated role with tasks set out in the GDPR, including responsibility for monitoring compliance with the GDPR. By Art. 37 GDPR, a DPO must be appointed where:

    (a) The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

    (b) The core activities of the controller or the processor consist of processing operations which "require regular and systematic monitoring of data subjects on a large scale"; or

    (c) The core activities of the controller or the processor consist of processing on a large scale of "special categories of data" pursuant to Article 9 (e.g. revealing race or ethnic origin, political opinions, religious or philosophical beliefs) and personal data relating to criminal convictions and offences referred to in Article 10.

39. Article 37 does not establish the precise credentials DPOs must carry, but does require that they have "expert knowledge of data protection law and practices." The GDPR's recitals suggest the level of expert knowledge *"should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor."*

40. A company with multiple subsidiaries or group of public authorities (a "group of undertakings") may appoint a single DPO so long as he or she is "easily accessible from each establishment." The GDPR also allows the DPO functions to be performed by either an employee of the controller or processor or by a third party service provider.

41. The DPO's tasks are delineated by Art. 39 of the GDPR and include: (a) informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws; (b) monitoring compliance with the GDPR and other data protection laws; (c) advising with regard to data protection impact

assessments when required under Art. 35; (d) working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data; (e) being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

42. Under the GDPR DPOs have many rights in addition to their responsibilities. They may insist upon company resources to fulfil their job functions and for their own ongoing training. They must have access to the company's data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line "to the highest management level" of the company. DPOs are expressly granted significant independence in their job functions and may perform other tasks and duties provided they do not create conflicts of interest. The GDPR expressly prevents dismissal or penalty of the DPO for performance of his or her tasks and places no limitation on the length of this tenure.

Penalties

43. Article 82 of the GDPR states that: *"Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."*

44. The GDPR establishes a tiered approach to penalties for breach[21]. There was much debate over the maximum level of fines that should be issuable. It was eventually agreed that a supervisory authority may impose fines for some infringements of up to €20m or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher for certain categories of breaches (e.g. breach of the requirements relating to the basic principles of processing, such as conditions for consent). Other specified infringements attract a fine of up to 2% of annual worldwide turnover. Article 83(2), GDPR, establishes a specific list of points to consider when imposing fines (such as the nature, gravity and duration of the infringement).

45. This is understandably one of the more controversial aspects of the GDPR and marks a significant departure from the present position where the ICO only has the authority to issue fines of up to £500,000 for serious contraventions of data protection laws.

[21] Art. 83, GDPR

46. This, together with the new breach notification provisions (see above), will no doubt see an increase in data subjects taking legal action against data controllers as a result of data breaches. It may even lead to more class actions like the one against the London Borough of Islington in 2013 when 14 individuals settled for £43,000 in compensation after their personal data was disclosed without their authority[22]. This action followed an ICO investigation that resulted in the council being fined £70,000.

Conclusion

47. The reforms introduced by the GDPR promise to be the biggest shake up for consumers' data protection rights for three decades. While many of the concepts and principles in the GDPR are the same as those currently in UK law, new elements and significant enhancements mean organisations will have to do some things differently.

48. In light of this, it is imperative that businesses and public authorities actively consider now what structural, technological and policy changes need to be introduced to ensure they are fully compliant by 26 May 2018. The threat of a significant financial penalties means that organisations simply cannot afford to fall behind. To that end the ICO has provided some guidance about what steps should be taken now to prepare for the GDPR[23].

Rhys Hadden
Guildhall Chambers
23 May 2016

[22] See http://www.islingtontribune.com/news/2013/dec/town-hall-data-breach-victims-set-receive-compensation-payouts-%C2%A35k (accessed on 23 May 2016)
[23] See: https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf