Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10
Email : ccbe@ccbe.eu – www.ccbe.eu

CCBE Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR)

19/05/2017

With this paper the Council of Bars and Law Societies of Europe (CCBE)[1] wishes to provide an overview of the main new compliance measures that Bars and Law Societies may wish to recommend in order to ensure compliance with the requirements set out in the GDPR.

In the following parts those aspects of the GDPR are highlighted that cause new or increased compliance responsibilities for, in particular, lawyers or law firms (hereinafter together referred to as a "law practices"). The purpose of so highlighting these matters is to seek to enable law practices easily to identify issues that should be of primary concern to them. Considering that the vast majority of European law practices are below the 250 employee threshold, the issues outlined below do not address provisions that apply to larger law firms only (for example, the requirement to have a data protection officer). Also, attention is drawn to the fact that many law firms process personal data that qualify as 'special categories of personal data'.

A. Security breach notification

According to Article 33, a law practice acting as data controller must notify personal data breaches to the supervisory authority without undue delay, and in any event not later than 72 hours after having become aware of such a breach. Any later notification is required to give reasons for the delay. There is an exception where the data breach is unlikely to result in any harm to the data subject(s).

If the law practice acts as a processor, it must also notify the controller without undue delay after becoming aware of a personal data breach.

The notification requires to contain, among other things, specification of the nature of the data breach (categories and approximate number of data subjects and personal data records concerned), the likely consequences of the breach and the measures taken or to be taken to mitigate the possible adverse effects. The notification can be made in different phases.

Furthermore, the controller is required to document such breaches in a sufficiently detailed manner, so that the supervisory authority can verify compliance with the breach notification. Law practices also require to establish internal procedures for handling data breaches, and to establish a mechanism for notification to the supervisory authority.

[1] The CCBE represents the Bars and Law Societies of 32 member countries and 13 further associate and observer countries, and through them more than 1 million European lawyers.

In certain high risk cases, the law practice is also required to notify its clients directly (Article 34), though there are special exemptions.

Clearly, the actual format of notification, the definition of "undue delay", the requirements as to content of the documentation and the interpretation by supervisory authorities of the thresholds and exemptions may well vary greatly among individual member states.

Therefore, law practices should be informed of any already existing and possible future national guidance in these areas.

Although some Member States have already implemented data breach reporting requirements in their respective national laws, Directive 95/46/EC did not oblige controllers to report data breaches to the supervisory authority. However, such a requirement already exists in the telecommunications sector (see Directive 2002/58/EC and Commission Regulation (EU) 611/2013, both applicable to providers of electronic communication services). The latter implementing regulation was defined in a sector independent way, and in some Member States, there may also be more detailed guidance issued by the telecom or data protection supervisory authorities. More importantly, based on this legislation, the Article 29 Working Party of the European Union data protection supervisory authorities has also issued detailed guidance on the implementation of the data breach regulation (WP 213 Opinion 03/2014 on Personal Data Breach Notification, 25 March 2014[2]) which sets out good practice in this area for all data controllers.

As for the future regulations in this area, under the GDPR Article 70(1) (g) and (h), the European Data Protection Board will also be likely to issue guidelines, recommendations and best practice for a) establishing breaches, b) determining "undue delay", c) circumstances in which a controller or a processor is required to notify the supervisory authority or its clients of the breach.

B. Right to be forgotten

Article 17 includes the right to erasure ('right to be forgotten'), which means that data subjects have the right to obtain from the controller the erasure of personal data concerning them without undue delay. The same article imposes upon the controller the obligation to erase personal data without undue delay if any of the grounds described in paragraph 1 point (a) to (f) applies. This provision has a history in the case of **Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González[3], where the Court stated that** individuals have the right (subject to certain requirements and safeguards) to ask search engines to remove links with personal information about them. However, paragraph 3 point (e) of article 17 includes an important restriction which may be invoked by law practices to the extent that their processing activities are necessary "for the establishment, exercise or defence of legal claims".

It is important to note that this obviously does not override certain local obligations to retain data for a certain period of time (for example to comply with tax obligations).

---

[2] Available under this link: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[3] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d57637cb18820e4ceb913ecf71af33028d.e34KaxiLc3qMb40Rch0SaxuTahn0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1115616

C. Data protection officer (DPO)

Obligation of law firms to appoint a DPO

Another new feature is the requirement to appoint a DPO if the data processing activities of an organisation involve regular and systematic monitoring of data subjects on a large scale, or processing of special categories of data on a large scale (article 37). The Article 29 Working Party (WP29), which is made up of representatives from the EU Member State data protection authorities, issued Guidelines on DPO's to clarify their role and provide best practice recommendations.

If a DPO is appointed, the organisation must publish the details of the DPO, and communicate those details to the relevant supervisory authority.

Under Article 9 of the GDPR, special categories of personal data are defined[4], the processing of which are prohibited, but with some exceptions: by way of Article 9 paragraph 2(f), the prohibition does not apply to data processing necessary for "establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity". Therefore, this provision validates the processing of special categories of data in the context of contentious legal work by law practices.

Nevertheless, Article 37 (and also Article 35, see below) still applies to the controller and the processor of special categories of data. These provisions require *designation of a data protection officer* in any case where the core activities of the controller or the processor consist of the processing on a large scale of special categories of data pursuant to Article 9. According to the Guidelines on DPO's, "'Core activities' can be considered as the key operations to achieve the controller's or processor's objectives. These also include all activities where the processing of data forms an inextricable part of the controller's or processor's activity".

The meaning of "large scale" is an important issue, because a smaller law firm may have cases with a large amount of data. However, it may be easy to argue, on the basis of recital 91 that this requirement will not apply to solo practitioners (see below under D regarding impact assessments).

Obligations and tasks of the DPO

The GDPR imposes important obligations to DPO's, such as the requirement to monitor compliance with the regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor, including responsibilities, obligations of awareness-raising and training of staff involved in processing operations, and the carrying out of related audits. The DPO's also act as a contact point for the data protection authorities.

The designated DPO, whether or not an employee of the law practice, should have an expert knowledge of data protection law and be able to fulfil all of the tasks based on Article 39 of GDPR, such as maintaining documentation of all processing operations, monitoring their implementation and the training of staff, the carrying out of audits etc. Therefore, a person who acts as a DPO will assume important and heavy responsibilities.

Lawyers acting as DPO's

It might be thought that a lawyer would be the person most suited to be appointed as a DPO, but it should be borne in mind that, having regard to the diversity of the duties required by this regulation, a person who is to be appointed as a DPO will require more than legal expertise alone.

---

[4] I.e. "[…] data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation […]".

The assimilation of the two functions (lawyer/DPO) and the risk of confusion between these functions are a key point for any lawyer who might be appointed as a DPO at the request of a client. A lawyer who is placed in such a position may find that he will need to alternate between the DPO function and the function of a lawyer exercising a regulated profession. A lawyer acting in the capacity of a DPO will require to ensure independence, and to avoid conflicts of interest, especially those conflicts which may arise from being simultaneously the contact person for the data protection authority (a role which involves obligations to report to the authority even if it is against the interest of the controller or processor) whilst also having a requirement to represent the clients' interests to the full extent permitted by law. In view of this potential conflict of interest, Bars and Law Societies may wish to recommend lawyers to assume such a responsibility of a DPO for an external client only if they have neither acted as a lawyer in matters which might fall within the DPO's responsibility nor will act, during their term as DPO, as a lawyer in matters they were or are involved in as DPO.

D. Impact assessments

According to Article 35, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, including any processing on a large scale of special categories of data, the controller must, prior to the processing, carry out an impact assessment (in particular when using new technologies, considering the purposes of processing etc.).

It is important to note that in recital 91, it is explained that the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from clients by an individual lawyer. This is an exemption which is clearly applicable to sole practitioners, but nonetheless, even a small law practice could still be required to deliver such impact assessments from time to time.

The problem is that according to the currently existing (non-sector specific) standards of data protection impact assessment frameworks, such an impact assessment could be prohibitive for small practices. For example, even a mere requirement of data controllers to identify software and hardware assets on which personal data rely could be interpreted by certain authorities as a requirement to implement a configuration and change management system. Generally, small practices with a few employees (but which are above the "individual lawyer" threshold) are generally not in a position to clearly comply with such requirements in the strict sense in all cases. A change management system would require a controlled and mature way of operation of their IT system which is usually not characteristic of practices of this size (it is very different to have a rough overview of the IT components the practice has, compared to having a working and controlled configuration and change management).

Unfortunately, neither the WP29 Guidelines on Data Protection Officers ('DPO's') adopted on 13 December 2016, nor the currently available draft WP29 Guidelines on Data Protection Impact Assessment (DPIA) provide any more guidance in this regard. Regarding recital 91, footnote 14 of the Guidelines on DPO's points out that everything between processing by an individual lawyer and processing of data of a whole country, is a grey area. This vagueness will unavoidably lead to different interpretations. [5]

Although this constitutes a new burden on law practices, by conducting impact assessments the regulation hopes to make it possible for law practices to be able to identify and address risks that would otherwise not have been detected, and prevent breaches that might otherwise have occurred.

[5] Since, at the time of writing, the Article 29 Working Party is still gathering comments from stakeholders on its draft Guidelines on Data Protection Impact Assessment (DPIA), a revised and final version might be published in the course of 2017 with possibly some further clarifications on what constitutes 'large scale' in respect of processing activities.

Compared to data breach notification, there is no clear regulatory history or guidance on how impact assessments should be conducted by law firms or other similar professionals.

Currently, data protection impact assessments are diverse in their content and methods, and are mostly popular in countries with common law traditions.[6] In Europe, the Information Commissioner's Office of the United Kingdom issued in 2014 a "*Privacy Impact Assessment Code of Practice*"[7] (following the "*Privacy impact assessment manual*" that was already published in 2007), and the French data protection authority (CNIL) published a "*Privacy Impact Assessment Manual*" in 2015[8]. Also, the European Commission issued a recommendation calling for impact assessment in relation to radio frequency identifier chips (RFID chips),[9] which resulted in an industry agreement of 12 January 2011, "*Privacy and Data Protection Impact Assessment Framework for RFID Applications*". This latter framework has been approved by WP29, and has also served as a model for a similar "template" initiative for smart meters.[10]

Unfortunately, these recommendations are specific to their subject matter and are unlikely to be of use as providing practical guidance for impact assessment by lawyers or similar professionals in the context of data breach notification. More details are to be expected from national, sector specific rules, if there will be any.

The results of a Commission funded privacy impact assessments study (Privacy Impact Assessment Framework for data protection and privacy rights) may be of some help to lawyers interested in the general background of privacy impact assessments.[11]

In summary, although the regulation itself goes into some detail with regard to impact assessments, the actual practical requirements are not yet known. Supervisory authorities and the aforementioned Board are expected to provide further guidance on the missing details, such as in relation to the kind of processing operations in which such impact assessments may be required.

E. Data portability

Data subjects have a right to obtain from the controller a copy of the personal data pertaining to them that is being or has been processed. Article 20 of the Regulation requires that such data should be handed over in a structured, commonly used and machine-readable format, but these are only very generic requirements.

According to the WP29 Guidelines on the right to "data portability", the terms "structured", "commonly used" and "machine-readable" are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. The WP29 guidelines also indicate that given the wide range of potential data types that could be processed by a data controller, the GDPR does not impose specific recommendations on the format of the personal data to be provided.

Although the requirement of commonly used and machine readable formats are easy to meet, the question of being "structured" can become a considerable issue. The documents lawyers use are usually unstructured in their content (for example Microsoft Word or PDF formats). There is no universally accepted format for handing over complete court files or cases in a structured format.

---

6 Environment impact assessments originally from the US are assumed to be the basis of privacy impact assessments, see the D1 deliverable of PIAF at http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf.

7 See https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

8 See https://www.cnil.fr/fr/node/15798.

9 See Commission Recommendation 2009/387/EC, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF.

10 See Commission Recommendation 2012/148/EU and its approval by the WP 29 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

11 http://www.piafproject.eu/About%20PIAF.html

All lawyers know how to hand over files to law firms newly appointed by their former clients, but sometimes the exact format and structure of such handing over is already an area where disputes between lawyers may arise. In the future, this issue may need further regulation by Bars and Law Societies.

F. Capability to track recipients of personal data

Data controllers have an obligation to be able to track recipients of personal data pertaining to a specific person (at a minimum, name and electronic contact details). This is also an obligation which often could be met by many law practices only if certain changes are made in their IT systems (for example, configuring the system in such a way as to have a reliably trackable record of recipients of personal information).