DRAFT CCBE Implementation Guidance Note regarding the General Data Protection Regulation (GDPR)

Introduction

The GDPR[1] was published on the 4th of May in the Official Journal of the European Union, with an implementation deadline of 6th of May 2018. Even though it is a regulation, important national differences could arise that affect how lawyers should work. Therefore, the CCBE would like to explain some of these possible differences, so that Bars and Law Societies can prepare to mitigate negative results of these differences.

The first part of this paper addresses the various measures that Bars and Law Societies are invited to consider regarding the national implementation of the new GDPR in order to ensure compliance with the principles of professional secrecy and legal professional privilege (PS/LLP). The second part provides an overview of ~~possible~~ the main new compliance measures that lawyers need to take to fulfil the requirements set out in the GDPR.

Part I: Recommendations regarding the national implementation of the GDPR

A. Legal basis for processing of personal data in the course of the activities of lawyers

Bars and Law Societies are advised to ensure that their government provides for a specific legal basis for the general processing of personal data by lawyers. According to the GDPR, the processing of personal data is only allowed unless the data subject has given consent to the processing, or if the processing can be based on any other legal basis listed in Article 6. This Article does not contain an explicit legal basis for the processing of personal data in the course of the activities of lawyers. However, according to Article 6 paragraph (1) point (e) and Article 6 paragraph (2), Member States may adopt provisions specifying under which circumstances the processing of personal data may take place "for the performance of a task carried out in the public interest":

- Article 6(1) point (e): *"Processing shall be lawful only if and to the extent that at least one of the following applies: […] processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."*
- Article 6(2): *"Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX."*

It is widely recognized that activities undertaken by lawyers, especially as regards contentious legal work, serve the interest of the administration of justice as well as the interests of those whose rights and liberties need to be asserted and defended. It is therefore in the public interest to introduce specific provisions setting out the legal basis and requirements for the processing of personal data in the course of the activities of lawyers related to contentious legal matters. Activities of lawyers involving non-contentious legal work might not be covered by such a public interest exception. Therefore, Bars and La Societies are advised to inform their members to seek consent from their clients when processing personal data in the context of non-contentious legal work.

It is assumed that for the processing of special categories of personal data, article 9(2) point (f) provides a sufficient legal basis for lawyers in relation to contentious legal work:

- Article 9(2) point (f): *"Paragraph 1 shall not apply if one of the following applies:-[…] (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;"*

B. Restrictions to information and access to personal data protected by PS/LPP

Paragraph 5 of Article 14 provides for ~~The only article that makes~~ an explicit exception to the information requirements of the controller where personal data have not been obtained from the data subject, in case the data are covered by PS/LLP. ~~of the applicability of the requirements set out in the GDPR for lawyers, is Article 14(5).~~ In particular, Paragraph (5) ~~of Article 14~~ restricts the application of ~~its~~ the first 4 paragraphs of Article 14 (regulating information to be provided where personal data have not been obtained from the data subject) *"where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union of Member State law, including a statutory obligation of secrecy"*. Therefore, when a lawyer in the course of his professional activities has e.g. collected data from a client about a third party, he or she is not required to fulfill the information requirements set out in Article 14 paragraph (1) to (4).

Furthermore, Article 23 restricts the scope of the obligations and rights provided for in Articles 12 to 22 *"when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: […] (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions"*.

This article may be used by Bars and Law Societies to ensure that Member States, in order to protect information covered by PS/LPP, apply adequate restrictions to the following articles:

- Article 13: "Information to be provided where personal data are collected from the data subject"
- Article 15: "Right of access by the data subject"
- Article 16: "Right to rectification"
- Article 17: "Right to erasure ('right to be forgotten')". In this regards it is important to note that paragraph 3 point (e) already includes a restriction which may be invoked by lawyers in relation to processing activities that are necessary "for the establishment, exercise or defence of legal claims". Bars and Law Societies may wish to ensure that this exemption is broadened to the extent that it also covers non-contentious legal activities of lawyers involving the processing of data covered by PS/LLP.
- Article 18: "Right to restriction of processing"
- Article 19: "Notification obligation regarding rectification or erasure of personal data or restriction of processing"
- Article 20: "Right to data portability"
- Article 21: "Right to object"
- Article 22: "Automated individual decision-making, including profiling"

~~***Question: Is it necessary to ensure restrictions for all these articles?***~~

C. Restrictions of the powers of supervisory authorities

Bars and Law Societies are invited to consider the option of restricting the power of supervisory authorities to access data held by lawyers, including their premises, in accordance with Article 90 GDPR (see also recital 164). This provision enables Member States to adopt specific rules setting out the powers of the supervisory authorities (as laid down in Article 58 GDPR) in relation to lawyers, as follows:

> "**Article 90**
>
> Obligations of secrecy
>
> *1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.*
>
> *2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them."*

Bars and Law Societies may therefore wish to urge their governments to ensure that the powers of the supervisory authority under Article 58 paragraph (1) point (e) and (f) ~~are restricted~~cannot be exercised without the consent of the relevant Bar or Law Society, as follows ~~in the following way~~:

> ***In case the controller or the processor is a lawyer and the supervisory authority wishes to use its powers under article 58 paragraph (1) points (e) and (f) to obtain access to all personal data and to all information necessary for the performance of its tasks, and to any premises of the controller and the processor, including to any data processing equipment and means, the supervisory authority is obliged to seek consent from the lawyer's relevant Bar or Law Society. When seeking consent, the supervisory authority must set out the reasons for its request, including the measures it will take to reconcile the right of the protection of personal data with the obligation of secrecy. Without the consent of the Bar or Law Society, the supervisory authority is not allowed to invoke its powers under Article 58(1) points (e) and (f) GDPR.***

D. Sanctions and enforcement

Article 83includes sanctions with higher amounts and percentages than the current privacy framework. These administrative fines can be up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. the imposition of such fines can have a very significant impact onindividual lawyers or law practices with a few employees.

Therefore, with regard to the national execution of the GDPR, Bars and Law Societies are invited to try to limit the upper amount of exposure faced by law practices.

Part II: Checklist of possible compliance measures for lawyers

The purpose of the following part is to highlight those aspects of the GDPR that cause new or increased compliance responsibilities for, in particular, lawyers or a law firms (hereinafter together referred to as a "law practices") so as to enable them to quickly identify the issues that are of their primary concern. Considering that the vast majority of European law practices are below the 250 employee threshold, the issues outlined below do not address provisions that only apply to larger law firms (e.g. a requirement to have a data protection officer). Also, attention is drawn to the fact that many law firms process personal data that qualifyies as ~~sensitive~~ 'special categories of personal data'.

A. Security breach notification

According to Article 33, a law practice acting as data ~~The~~ controller ~~shall~~ must notify ~~the~~ personal data breach~~es~~ to the supervisory authority with undue delay, not later than 72 hours after having become aware of it. ~~(~~Any later notification shall contain 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 contains among other things, 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. Based on the lack of details, law practices have to set down internal procedures for handling data breaches, and also to establish a mechanism for the notification to the supervisory authority.

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

Clearly, the actual format of notification, the actual definition of "undue delay", the content of the documentation and the ways how supervisory authorities and law practices interpret the thresholds and exemptions could and will vary greatly among countries.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available here.

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

Although some Members States 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 ~~The~~ requirement ~~of data breach notification~~ is already existing under 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 rather sector independent way, and in some countries, there may also be more detailed guidance issued by the telecom or data protection supervisory authorities. More importantly, based on this legislation, Article 29 Working Party of the European Union data protection supervisory authorities has also issued a 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 presents good practices for all controllers.

As for the future regulations in this area, under the GDPR Article 70(1) point (g) and (h), the European Data Protection Board will also issue guidelines, recommendations and best practices 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, as already pointed out in Part I.B above, 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". ~~According to Article 17 (3), the regulations mentioned above shall not apply to the extent that processing is necessary for *the establishment, exercise or defence of legal claims*.~~ ~~Needless to say, it is important that this exemption is not narrowed down in scope in member states when being implemented.~~

C. Data protection officer (DPO)

Obligation of law firms to appoint a DPO

Another novelty concerns the requirement to appoint a DPO if the data processing activities of an organisation involves regular and systematic monitoring of data subjects on a large scale, or processing of special categories of data on a large scale (article 37). If a DPO is appointed, the organisation must publish the details of the DPO, and communicate them to the relevant supervisory authority.

[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

Under Article 9 of the GDPR, special categories of personal data are defined[4], the processing of which are prohibited, but with some exceptions; ~~under Section 2. B~~by way of Article 9 ~~Section~~ paragraph 2 point (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 processing on a large scale of special categories of data pursuant to Article 9.

The meaning of the "large scale" is an important issue, because a smaller law firm may also have cases with a large amount of data. ~~(~~Based on recital (91), it is easy to argue that this requirement will not apply to solo practitioners, see below under D ~~for Article 35~~regarding impact assessments~~)~~.

~~Powers~~ Obligations and tasks of the DPO

The GDPR grants important ~~new powers~~obligations to DPOs, such as monitoring 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 related audits. The DPOs also act as a contact point for the data protection authorities.

The designated DPO, whether or not an employee of the law practice, s~~h~~ould~~all~~ have an expert knowledge of data protection law and ~~shall~~ 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, audits etc. Therefore, acting as the DPO will become ~~a risky business~~an important responsibility.

Lawyers acting as DPOs

The lawyer seems currently the most competent to practice as a DPO. However, regarding the diversity of tasks provided by this regulation, being a DPO requires more than legal expertise.

The assimilation of the two functions (lawyer / DPO) and the risk of confusion between these functions are a key point for the lawyer practicing as a DPO. Such a lawyer will alternate between the DPO function and a regulated profession. The lawyer acting as a DPO has to ensure his/her independence, and avoid conflicts of interests, especially those stemming from being the contact person for the data protection authority (which also involves obligations to report to the authority even if it is against the interest of the controller or processor) versus representing its clients' interests as far as legally possible (similar to the double nature of an internal auditor of highly regulated markets).

D. Impact assessments

[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 […]".

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.). ~~Although~~

It is important to note that in recital ~~(~~91~~)~~ it is explained ~~states~~ that the processing of personal data should not be considered to be on a large scale ~~"~~if the processing concerns personal data from ~~patients or~~ clients by ~~an *individual* physician, other health care professional or a~~ lawyer.~~"~~ This is a clear exemption to solo practitioners, but nonetheless, a large ~~group of lawyers~~law practice could still be required to deliver such impact assessments from time to time. Although this constitutes a new burden on some law practices, by conducting impact assessments, law practices may be able to identify and address risks that would otherwise not have been detected, and avoid breaches that might otherwise have occurred.

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

Currently, data protection impact assessments are quite diverse in their content and methods, and are mostly popular in countries with common law traditions.[5] In Europe, it was the United Kingdom that first published a "privacy impact assessment manual" in 2007. Later, in Europe, the Commission issued a recommendation calling for impact assessment in relation to radio frequency identifier chips (RFID chips),[6] which resulted in an industry agreement of 12 January 2011 named "Privacy and Data Protection Impact Assessment Framework for RFID Applications". This framework has been approved by the Working Group 29 as well multiple times, and also served as a model for a similar "template" initiative for smart meters.[7] Compared to data breach notification guidelines, these recommendations and agreements are very specific to their subject matter and of no use as a guidance for impact assessment by lawyers or similar professionals.

The results of a Commission funded privacy impact assessment study (Privacy Impact Assessment Framework for data protection and privacy rights) can ~~also~~ be some help to lawyers interested in the general background of privacy impact assessments.[8]

In summary, although the regulation itself goes into some details of the impact assessment, 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 the "kind of processing operations" where such impact assessment is required or not.

E. Data portability

Data subjects have a right to obtain from the controller a copy of its personal data that is being 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.

The aforementioned European Data Protection Board or the authorities themselves may issue guidelines and recommendations in this regard, but they are not required by the Regulation to do so. 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 (e.g. Microsoft Word or PDF formats). There is no universally accepted format for handing over complete court files or cases in a structured format.

All lawyers know how to hand over certain files to law firms newly appointed by 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 (name and electronic contact details at minimum). This is also an obligation which can only be met if certain changes are made in the IT systems of law practices (e.g. having a reliable track record of recipients of personal information).

[5] 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.

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

[7] 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

[8] http://www.piafproject.eu/About%20PIAF.html