ETHICS WATCH

Maryland Ethics Committee Confronts the GDPR and Gets it Wrong

By Nathan Crystal and Francesca Giannoni-Crystal

As businesses and governments have increasingly moved from paper to electronic record keeping, privacy of personal data has become a topic of fundamental importance. For lawyers this development has important implications for their practices, both in terms of advising clients and practice management.

Compliance with privacy obligations was complicated enough before this year, but increased substantially when the EU General data Protection Regulation (GDPR) became applicable on May 25, 2018.[1] The GDPR applies to the "processing" of "personal data" of "data subjects" and has extraterritorial application, so that many American organizations (including law firms) are subject to it.[2]

When applicable, the GDPR imposes a number of obligations and grants data subjects several rights, including the right to erasure, commonly called the "right to be forgotten." GDPR Article 17.

Recently the Maryland State Bar Ethics Committee became what is believed to be the first U.S. ethics committee to deal with the GDPR. Maryland State Bar Assn. Ethics Op. #2018-06, available at www.msba.org/ethics-opinions/2018-06. The Committee responded to the following question: Can a lawyer simultaneously comply with both the duties regarding personal data imposed by the GDPR, including the right to erasure of personal data, when a former client makes this demand, and the lawyer's obligation under the Rules of Professional Conduct to determine and resolve conflicts of interest under Rule 1.7 (current clients) and 1.9 (former clients)?

The committee gave a Solomonic answer: An attorney can comply with both the GDPR and the ethics rules because the request of erasure works as a "waiver" of future conflicts of interest. A waiver results if the firm gives the client (1) a written explanation that if the firm complies with the request "the client consents to the firm's potential future representation of other clients with conflicts that might otherwise have been discovered, and (2) none of the attorneys who handle the matter for the firm have any retained knowledge of the former client's information."

Since this opinion appears to be the first U.S. ethics opinion dealing with the GDPR, it is unfortunate that the opinion is flawed in three respects: (1) scope of application of the GDPR, (2) attachment of "right to be forgotten" exception, and (3) inadequacy of the data subject's waiver to deal with conflicts of interest.

Scope of the GDPR

The Maryland Committee began its opinion correctly by focusing on when a controller or processor of personal data is subject to the GDPR. For the GDPR to apply, the firm must

> (1) process data "in the context of the activities of an establishment … in the Union" (Article 3.1); OR
> (2) "offer … goods or services" with an intent to target "data subjects in the Union"; OR
> (3) monitor "their behaviour as far as their behaviour takes place within the Union." Article 3.2(b).
>
> (It is not relevant here, but the GDPR applies also to the processing by a [non resident] controller …, but in a place where Member State law applies by virtue of public international law" Article 3.3).

A lawyer is almost always a "controller" of personal data because of the independence that characterizes the lawyer's activity (See Article 4(7) Definition of "controller").

Having identified the relevant provision on the GDPR's territorial scope (Article 3), the Committee, however, creates a misleading impression of its scope by accepting without discussion that the GDPR applies even when prospective or former EU Clients "submit information for purposes of engaging legal services." This is incorrect.

The evaluation of when there is an EU "establishment" for GDPR purposes or when there is a targeting and/or "monitoring" requires an "*in concreto*" evaluation. See the *EDPB's recent Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (version for public comment).[3] That evaluation is complicated[4], but certainly the mere submission of personal data by EU residents to a U.S. lawyer or firm is insufficient to subject a lawyer or firm to the GDPR.

Attachment of the "Right to be Forgotten" (Article 17)

The Committee stated that it was not authorized to render opinions on the GDPR, that there might be exceptions to the right to be left alone that would allow the lawyer to retain data, and if that was the case "no ethical issue" arises. While such a "disclaimer" is probably

technically correct, it produces a misleading opinion because with proper planning and with competent knowledge of Article 17, the lawyer could either avoid the right to attach or use exceptions to avoid application. Becoming familiar with the GDPR (or retaining counsel for advice on GDPR issues), as applicable to a lawyer's practice, is required by the duty of competence under Rule 1.1.

The "right to erasure" is not an absolute right. Understanding of the conditions of attachment of the right to erasure requires an understanding of GDPR concepts of "lawful processing" and "privacy notice." Article 6 of the GDPR provides that processing must be "lawful" (Article 6.1) and that this is the case only when one of the legitimate grounds for processing listed in Article 6.1(a) to (f) exists. Relevant for the processing performed by lawyers are most notably: consent, Article 6.1(a); contract performance, Article 6.1(b); and legitimate interest, Article 6.1(f). These grounds for processing, together with the specific purposes for which the data is processed (e.g., performance of the engagement agreement), must be specifically mentioned in the privacy notice required by Articles 13 and 14 of GDPR. See Article 13.1(c) and 14.1(c).[5] This notice (which must include many elements in addition to grounds and purposes of processing) should be properly drafted by lawyers with an eye to their ethical obligations.

Article 17.1 of the GDPR requires one of the following conditions to exist for the right to erasure to attach:

- the personal data whose erasure is demanded is "no longer necessary in relation to the purposes" of collection or processing; Article 17.1(a)
- the processing is based on consent, the consent is withdrawn and "there is no other legal ground for the processing"; Article 17.1(b)
- the data subject objects to a processing based on public interest or legitimate interest of and there are no "overriding legitimate grounds" for the processing; Article 17.1(c)
- the personal data have been "unlawfully processed" (i.e. processed outside one of the grounds listed in Article 6); Article 17.1(d)
- erasure is mandated by compliance with "a legal obligation in Union or Member State law"; Article 17.1(e) or
- the personal data "have been collected in relation to the offer of information society services" directed to minors. Article 17.1(f)

If a lawyer properly drafts the privacy notice for his/her clients, Article 17.1(a) almost never applies. The lawyer's privacy notice should specify "compliance with ethics rules" among the purposes for processing of client information; by specifying that, it is hardly possible that the personal data of a former client can become "no longer necessary in relation to the purposes."

Condition (b) based on withdrawn consent should also never apply because lawyers' processing of clients' (and former clients') data should not be based on consent (contract performance and legitimate interest are much better grounds) because consent as a ground for data processing can be withdrawn. Article 7.3.

Condition (c) should rarely if ever be applicable because – provided that the lawyer is processing the data of a former client on the basis of legitimate interest instead of consent - the lawyer should always have an "overriding legitimate grounds" for processing.

Unlawful processing under condition (d) should obviously never occur. We are unaware of legal obligations "in Union or Member State law" (outside of the erasure obligation in the GDPR) that would require a lawyer to erase former clients' data under condition (e). Lastly, condition (f) does not apply because lawyers' services are never "information society services" directed to minors.

If the erasure right has attached because of the occurrence of one of the above-mentioned conditions, a lawyer still has the ability to resist erasure on one of five exceptions listed in Article 17.3(a)-(e), which are all based on some necessity of processing. While the first four are probably never relevant for lawyers, the fifth is relevant: processing is necessary "for the establishment, exercise or defence of legal claims." Article 17.3(e). This exception could apply in two settings: (1) when a new client contacts the lawyer to be represented in his/her claim or defense, the possibility for the lawyer to check possible conflicts of interest with former clients is necessary to verify that the law firm can offer a conflict-free representation and hence foster the new client's "establishment, exercise or defence of legal claims"; (2) the new client could file an ethics complaint against the lawyer for violation of the duty to offer a conflict-free representation or could sue the lawyer for malpractice or breach of fiduciary duty. Also, a disqualification motion based on the assistance of that

former client could be brought. The deletion of a former client's records does not avoid this occurrence and on converse makes it more difficult (if not impossible) for a lawyer to defend himself/herself against an ethics complaint, a lawsuit or a disqualification motion because in the records that he/she deleted there may be important information such as the extent of the former client's representation, the information that the lawyer actually acquired, the date in which the representation ended – all elements that are lost forever from the deletion.

Inadequacy of the data subject's waiver

Assuming that the client (data subject) had the right under the GDPR to have his/her data erased, the Committee advised that the request would amount to a waiver of conflicts of interest if the client gave informed consent to the consequences of deletion of the data:

> In this case, if a lawyer or law firm gives the client a full explanation of the consequences if a client exercises its "right to be forgotten," including an explanation of the reasons why a law firm or attorney tracks client and matter information, and the client nevertheless gives written instruction to delete all of its data, we believe that the client has waived any conflicts that may arise in the future with respect to other clients and that may have been avoided by use of the deleted data.

The problem with this analysis is that the data subject "waiving" the conflict of interest is not the only client affected by the conflict. A new client that hires the firm after the erasure of data by the former client in a matter that is adverse to the former client has an interest in being informed of the firm's prior representation of the adverse party. The new client has the right to decide whether the prior representation is substantially related to the new matter, Rule 1.9(a), or whether the firm's prior relationship creates a "significant risk" that the representation of the new client will be "materially limited by the lawyer's responsibilities" to the former client, Rule 1.7(a)(2). The erasure of the data of the former client makes it difficult if not impossible for the firm to identify and inform new clients of possible conflicts of interest with the former client whose data has now been erased, except from the memories of the lawyers who represented the former client.

Moreover, other problems exist with the Committee's analysis: Under the Rules of Professional Conduct "waivers" of conflicts of interest require "informed consent," see Rule 1.7(b)(4) and 1.9(a). Waivers of unknown prospective conflicts of interest are of doubtful validity. See Rule 1.7, cmt. ("If the consent is general and open-ended, then the consent ordinarily will be ineffective, because it is not reasonably likely that the client will have understood the material risks involved."). Thus, the waiver by the former client is of questionable validity in a subsequent proceeding.

In addition, the Committee advised that it was also necessary that "none of the attorneys who handle the matter for the firm have any retained knowledge of the former client's information." This requirement would mean that if any attorney who handled the matter for the former client remained with the firm, the Committee's "waiver" analysis would not apply. In addition, contrary to the Committee's analysis, retention of information about a data subject in the memory of an attorney does not violate the GDPR because the GDPR does not apply. Article 2.1 states:

> This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. (emphasis added).[6]

Neither of these apply to retention of personal data in the memory of an attorney.

For these reasons the Maryland Committee was wrong in advising that a lawyer confronted with an assertion of the GDPR right to be forgotten could comply with the request by treating the request as a waiver of the right to claim a conflict of interest. Instead, the inquirer should have been reminded of his/her Rule 1.1 duty of competence, which would require the lawyer to do the following: first, to correctly analyze whether he/she was subject to the GDPR; second, if subject, to properly draft a privacy notice that included compliance with ethics rules as a purpose for processing; third, to point out to the former client requesting erasure that there are "overriding legitimate interests" (compliance with ethics rules) that oppose the request; and fourth, to raise the exception of Article 17.3(e) (i.e., that processing is necessary for the "establishment, exercise or defence of legal claims").

Endnotes

[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 at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[2] "Processing", "personal data", "data subjects" (together with other important concepts such as "controller" and 'processor") are defined terms. See Article 4 (Definitions).

[3] *EDPB's recent Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (version for public comment), available at https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en

[4] The analysis is difficult, among other reasons, because the term "establishment" (Article 3.1) is not defined by the Regulation and neither are the "offering of goods and services" or "monitoring". Clarifications, however, are given in Whereas [22], [23] and [24].

[5] The privacy notice must be provided at the time of data collection "where personal data relating to a data subject are collected from the data subject" (Article 13.1) and "within a reasonable period after obtaining the personal data" Article 14.3.

[6] On this see also Whereas [22] that specifies: "Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation."