CNA

We can show you more.®

PROFESSIONAL COUNSEL℠

ADVICE AND INSIGHT INTO THE PRACTICE OF LAW®

GDPR + U.S. Law Firms = An Important Moment For Introspection

A CNA PROFESSIONAL COUNSEL GUIDE FOR LAWYERS AND LAW FIRMS

Introduction

On May 25, 2018, the General Data Protection Regulation ("GDPR") became effective in all European Union ("EU") Member States. It is the most significant revision to data protection regulations in the EU since the 1998 Data Protection Act. Much has been written about how the GDPR applies to businesses that are either located in the EU, do business with EU residents or those that simply collect and process data of EU residents. This article will focus on how new data protection requirements set forth in the GDPR may affect small and mid-size U.S. law firms that represent clients "in the EU."

It is incumbent upon law firms that "passively" conduct business with EU residents to acknowledge this activity and do so purposefully and in compliance with the GDPR. Failure to do so may be shortsighted because a growing list of countries are developing data protection laws similar to the requirements imposed by the GDPR, such as Japan, China, Korea, and Canada.[1] In addition, the California legislature recently enacted the California Consumer Privacy Act ("CCPA") of 2018, which adopts many similar GDPR-type accountabilities. The CCPA will become effective on January 1, 2020. In other words, data privacy and security is the new normal. Even law firms that do not conduct any business in the EU would be well served to begin developing law firm policies and procedures that incorporate privacy by design.

Law firms hold a large volume of confidential client information as well as personally identifiable information, making them a target rich environment for cyber criminals. In addition, law firms typically retain documents throughout lengthy representations and for years thereafter. CNA has published a number of articles highlighting professional liability risks when firms fail to comply with state rules of professional conduct relating to unauthorized disclosure of client information and emphasizing the need to develop robust document retention policies and data collection practices.[2] The GDPR presents additional accountabilities that firms must address when engaging in certain activities. So, the first inquiry is, "does the GDPR apply to your practice?"

Application of the GDPR

The GDPR is focused on protecting the rights of data subjects, or the natural person in question, when certain information is processed by a third party. So, while the regulation clearly applies to law firms[3] in the EU that process EU residents' data, it also applies to law firms outside of the EU in certain circumstances. This extra-territorial scope of the regulation is found in Article 3.2:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) The monitoring of their behavior as far as their behavior takes place within the Union.

1 Sanderson, Heather, Bortnick, Richard, Vollweiler, Cheryl, and Wrynn, James, *The Effect of the GDPR on American and Canadian Business,* For the Defense, DRI (May 2018).
2 These articles are available at **www.cna.com/lawyersriskcontrol**.
3 While the GDPR applies to businesses beyond law firms, this article will focus on law firms when discussion applications.

There are a couple of pieces to digest in this part of the regulation. First, the regulation applies when the data subject is "in the Union…." Keep in mind, the scope of the regulations is not limited to individuals who are citizens of Member States in the EU. Technically, it even includes citizens from any country who are merely passing through the EU while on vacation.[4] The regulation provides protections for all natural persons while in the EU.

Second, the regulation applies to the processing of "personal data" by a controller or processor.[5] In the United States, law firms have been focused on protecting "personally identifiable information ("PII")" as defined by various state data breach notification laws. Typically, PII includes an individual's name together with an identifying field such as social security number, driver license number, financial account number or similar information. The GDPR expands the class of protected information to include any information relating, directly or indirectly, to an identifiable natural person such as individual's Internet Protocol address ("IP address"), location data, or even political or religious affiliations.[6]

Taking a pause, does the scope of the GDPR include anyone in the world, even U.S.- based family members who store an EU resident's name and address in their personal contacts folders? No, the GDPR does not apply to processing in the course of exclusively personal or household activities.[7] The extra-territorial scope of the GDPR is limited to controllers or processors who either 1) offer goods or services in the EU or 2) actively monitor natural persons behaviors while those persons are in the EU.

Therefore, family members in the U.S. are not required to hire a contractor to ensure that their home computers are GDPR compliant. On the other end of the spectrum, large U.S. multi-national social media corporations have been undergoing years of revisions to their business processes to ensure compliance. U.S. based law firms fall in between these two poles.

The GDPR should not apply to U.S. firms practicing domestic law that do not actively market themselves to potential EU clients and that do not actively monitor EU residents.[8] However, consider a firm that receives social media data of an EU resident who happens to be a witness in a domestic U.S. matter. Again, the GDPR probably does not apply because the firm is not actively engaged in offering services in the EU or is not actively monitoring the individual, although the firm may be required to certify it is Privacy Shield compliant, or execute Model Clause to transfer data to the United States.[9] What if the firm begins to actively market U.S. domestic patent services to EU clients through its website? What if a family law firm actively markets services to high wealth individuals who have seasonally relocated to the EU and the firm accepts payment in Euros? What if an immigration firm markets through its website, which is translatable into various EU dominant languages, and routinely communicates with new clients and relatives in the EU? The firms in these latter examples will probably be subject to GDPR requirements.

4 Sanderson, Heather, et al., *The Effect of the GDPR on American and Canadian Business*, For the Defense, DRI (May 2018).
5 Generally, a controller determines the purpose and means of the processing of personal data and a processor simply processes the data on behalf of the controller. For specific definitions see GDPR Art. 4.7 and Art. 4.8, as well as related duties in Art. 24 and Art. 28, respectively.
6 *See* GDPR Article 4.1.
7 *See* GDPR Recital 18.
8 Garrelfs, Alexander, *GDPR Top Ten: #3 Extraterritorial Applicability of the GDPR*, Deloitte (April 3, 2017). *See* **https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-top-ten-3-extraterritorial-applicability-of-the-gdpr.html**
9 *GDPR: Ready or Not…!*, Association of Corporate Counsel Presentation (May 2, 2018).

So what exactly is required by the GDPR? The GDPR[10] reads similar to a typical U.S.-enacted regulation, with various Chapters and Articles. Some Articles provide very specific duties and requirements. Other Articles expressly grant rights to data subjects which, in turn, impose less clear obligations on those processing data. A good resource for compliance with the GDPR is the Information Commissioners Office ("ICO") in the United Kingdom: https://ico.org.uk. The ICO is the UK independent authority that enforces information rights and data privacy for individuals. According to the website, GDPR compliance for small businesses should be manageable because "[a] lot of the rules and themes of the new data protection law are just building on what is already in the current law so it is not a complete change…." The website offers several data protection self-assessment toolkits on the topics of controller and processor accountabilities, information security, records management and data sharing, among other topics.

Law firms are encouraged to take advantage of the resources available from the ICO and, in addition, to retain legal counsel or a specialized vendor to confirm that the firm's processes are compliant with the GDPR. The scope of this article is simply to highlight new requirements imposed by the GDPR that are most relevant to small and mid-size firms, and to provide general risk control recommendations to enhance general law firm data privacy workflows. The article is not a playbook for complying with GDPR requirements. Rather, the practices recommended here simply make good business sense in bringing law practices further into the modern digital age.

Client Intake: Updates to Privacy Policies and Engagement Letters

To enhance transparency in law firm data privacy controls, law firms should consider adopting two new strategies during the initial client intake process: adopting and disclosing a data privacy policy (which the GDPR describes as a "privacy notice") and updating engagement letters to include a consent-to-process provision or a "legitimate interests" notification.

Privacy Policy Updates

Article 24(2) of the GDPR requires that a law firm's technical and organizational measures be defined in a data protection policy. While many vendors or data security lawyers will be able to craft personalized policies for individual firms, there are many resources available to help firms develop their own data protection policies as well.[11] Generally, the GDPR requires data privacy policies to contain, at a minimum, the following information:

- Recipient(s) of personal data
- Legal basis for processing (e.g. consent or legitimate interest)
- Data retention period
- Data Subject's right to correct, erase, restrict processing of personal data
- Data Subject's right to withdraw consent
- Data Subject's right to lodge complaint with supervisory authority

10 A link to the formal EU website discussing the GDPR https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

11 For example, the International Association of Privacy Professionals offer guidance (https://iapp.org/resources/article/sample-data-protection-policy-template-2/). *See Also* U.K.'s Information Commissioner's Offices (https://ico.org.uk).

It is recommended that a copy of the firm's data protection policy be provided to new clients and be readily available for current clients. In addition, law firms should include a data privacy notice on websites. Examples of privacy notices can be accessed through the ICO website or, alternatively, examples may be found on websites of a number of major international law firms. Given the world-wide implications of these regulations, it is important to include this notice on websites.

In addition, if the law firm utilizes a "contact us" page that accepts direct communications from website users, then the firm should update the disclaimer language if the firm will not be soliciting EU data subjects. While "disclaiming" solicitation from EU data subjects will not ensure exemption from the scope of the GDPR, it will help to provide a good faith basis in defending a potential sanction proceeding.

Recently, it was reported that Tronc, Inc., which owns the *Los Angeles Times* and *Chicago Tribune*, went to the extreme step of blocking all website users with European IP addresses from accessing its content out of concerns emanating from GDPR compliance.[12] While small and mid-size firms will probably not possess the technical or financial resources to block the entire EU population, including the following language will at least focus the intent of the law firm's targeted audience:

> Unsolicited emails and other information sent to [Law Firm] will not be considered confidential, may be disclosed to others, may not receive a response, and do not create an attorney-client relationship with us. If you are not already a client of [Law Firm], please do not send us any confidential information. In addition, this [Law Firm] is currently not accepting any new business from any data subject or other legal entity that may be within the scope and derive the benefits of the EU General Data Protection Regulation.

Engagement Letter Updates

In addition to updating the firm's data privacy policy, Chapter 2 (Art. 5-11) of the GDPR addresses processing of personal data. According to Article 5(1), Personal Data must be fairly and lawfully processed in a transparent manner. As it relates to law firms, Article 6(1) provides that processing shall be lawful only if the data subject has given consent for one or more purposes, or "if processing is necessary for the purposes of the legitimate interests pursued by the controller…." The purposes most likely applicable to law firms, in addition to consent and "legitimate interests" include when:

- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject; or,
- processing is necessary in order to protect the vital interests of the data subject or of another natural person.

If a law firm intends to use the personal information for any purpose other than that outlined in an engagement letter, it needs to make sure it obtains consent. The requirements for obtaining consent are delineated in Articles 7 and 8. Consent must be freely given, specific, informed and also should unambiguously demonstrate the data subject's intent to consent. Some practical recommendations for obtaining adequate consent include the following:

- Consent terms should be clear, unambiguous and easy-to-understand.
- Requests for consent should be separate from other terms in the engagement letter, or as an addendum or rider to the engagement letter for clarity and ease of tracking consent at later dates.

12 Moorcraft, Bethan, *LA Times and Chicago Tribune EU exit highlights complexity of GDPR*, Insurance Business America (July 10, 2018).

- If the representation requires you to process the data in a manner not originally disclosed in the client consent, then an updated consent clause must be obtained (e.g. court orders electronic discovery and the parties agree on the vendor not originally disclosed in original consent agreement).
- A clear opportunity for the client to affirmatively provide consent, either through a separate line for initialing or signing the agreed-to consent terms, or checking a box to "opt-in." Requiring the data subject to "opt-out," inferring a default "opt-in," is not adequate. It is also not adequate to infer consent simply because the data subject has not affirmatively provided consent over a certain amount of time.

Alternatively, law firms may assess if they may lawfully process data based on the "legitimate interests," basis in Article 6(1)(f). Recital 47 to the GDPR states the following:

> The legitimate interests of a controller…may provide a legal basis for processing provided that the interests or the fundamental rights and freedoms of the data subject are not overriding….***Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.*** At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. (emphasis added).

Notably, if the firm plans to rely on the legitimate interest basis for lawful processing, the firm remains obligated to notify the client in the engagement letter of this approach. A good summary of requirements when relying on legitimate interest has been developed by the Data Protection Network.[13]

These requirements emphasize the importance of securing properly signed engagement letters prior to receiving any client data or commencing work on a matter. CNA has previously emphasized the importance of engagement letters in several prior articles and also offers the *Lawyers' Toolkit 4.0*, which provides sample engagement letters and clauses. Receiving a client's data prior to receiving proper consent may be deemed a violation of the GDPR.

File Management: Updates to Internal Document Management and Record Retention Plans

Once the firm has adopted an appropriate data privacy policy and has taken steps to properly collect client data, the next step is to improve the process of actual data collection, processing, and ultimately destruction.

Internal Document Management

In addition to the right to withdraw consent at any time, the GDPR recognizes a variety of rights that are set forth in Chapter 3 GDPR (Art. 12-23) and, as relevant to typical law firm practices, are as follows:

- **The right to be informed:** The right to be informed on the who, what, when, why and where of the data being processed (Art. 12, 13, 14).
- **The right of access:** The right to receive confirmation that data is being processed and access to personal data upon request (Art. 15, 20).

13 Guidance on the use of Legitimate Interest under the EU General Data Protection Regulation, ver. 1.0 (October 7, 2017). *See Also* **https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf**.

- **The right to rectification:** The right to have personal data rectified if it is inaccurate or incomplete (Art. 16).
- **The right to erasure:** The right to have personal data erased and to prevent processing. This is also referred to as "the right to be forgotten." (Art. 17)
- **The right to restrict processing:** The right to request that a third party cease using personal data (Art. 18).
- **The right to data portability:** The right to have the ability to transfer personal data easily from one system to another in a safe and secure manner, without hindrance to usability (Art. 20).

It is important to understand the rights of clients, as recognized in the GDPR, because a law firm's document management processes must ultimately be able to honor those rights. Here are some tips to enhance a general law firm's data management processes:

- **Engagement Letters:** Law firms should consistently require engagement letters for every representation. Letters should properly define 1) the scope of the representation, 2) the purpose and use of information obtained during the engagement, 3) a description of the firm's document retention policy, and either 4) consent as necessary or legitimate interest for processing.
- **Develop a Record Management Process:** The process should include an opportunity to annotate the file whenever data is transferred from the firm to a third party and the purpose for the transfer (Art. 30) (e.g. opposing counsel-discovery, co-counsel-legal counsel, e-discovery vendor-compliance with court ordered discovery, expert witness-technical guidance, etc.). In addition, the process should ensure that the firm has the proper technical and administrative mechanisms to comply with the data subject's rights enumerated above such as access, erasure and portability.
- **Review Vendor Contracts:** Law Firms should review vendor contracts to reconfirm the data privacy and use-of-data provisions in those contracts. The GDPR imposes joint and several liability on controllers and downstream processors and may seek enforcement against any of these entities in a chain of custody (See Chapter 4, Art. 24-43). Accordingly, it is also important to negotiate indemnification and contribution terms with vendors who will be receiving client data directly from the law firm.
- **Caution in Litigation:** When disclosing client data during the discovery process, it is important to seek reasonable assurances of security from the opposing side. Today, it is not uncommon for parties to expressly stipulate to certain minimum security requirements as a condition to disclosure of data, either through a F.R.C.P. Rule 26(f) conference or analogous state rule.
- **Train Staff:** Article 24 states that a controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR requirements. Accordingly, law firms are encouraged to properly train and routinely retrain staff on the firm's records management processes.

Record Retention Policies

Law firms typically retain closed or dormant files for years after the conclusion of the representation for a number of reasons including:

- To defend a future potential claim for malpractice;
- To utilize certain form documents relating to the client in future representations;
- To enforce a client's future contractual or other legal position; or
- To comply with other legal requirements for file or data retention.

CNA recently published two Professional Counsel Guides to help law firms develop a record retention policy and to assist firms in managing disputes over file materials with the client.[14] In addition to the recommendations in those publications, law firms also should consider the concept of "data minimization" in developing record retention policies.

The concept of data minimization is espoused in Article 5(1)(c, e) and requires that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and shall be kept in a form which permits identification of data subjects for no longer than is necessary. Law firms should focus on carefully working with clients to manage the flow of unnecessary data into the firm. In addition, firms should properly cull file materials as part of the file close-out process in order to remove or redact personal client data.

In addition, consider the example of a long term client who unfortunately decides to move its files to a new law firm. The firm receives a letter with instructions on transferring files to the new firm. Included in that letter is also a demand that the current firm destroy all copies of the client's files, both open and closed, immediately after tendering the originals to the new firm. This complex issue is becoming a challenge for law firms. Most guidance on this subject by the American Bar Association and State Bar Associations relates to an attorney's right to keep a copy file materials at the attorney's own cost.[15] However, those opinions fail to address the attorney's right to a copy of the file, regardless of cost, if the client demands that the lawyer destroy the records: all except one, as of the date of this article.

The New York State Bar Association (NYSBA) issued *Ethics Opinion 780* in 2004. In this Opinion, the NYSBA concluded that both the client and the attorney have an interest in the file materials. An attorney's interests include the right to retain copies of the file in order to collect a fee or to defend against an accusation of wrongful conduct. If the client objects to the attorney's retention of copies, the NYSBA concluded that the attorney may insist on a general release as a condition of that agreement. The NYSBA acknowledged that a lawyer is typically prohibited from prospectively seeking to limit liability to a client for malpractice. However, there is no restriction on seeking a release for work already completed as contemplated here. The attorney also must instruct the client to seek independent counsel in the negotiation for the release. How this issue will continue to develop with the clients "right to be forgotten" provided in the GDPR will certainly be an issue to follow.

14 *See Creating a File Retention and Destruction Policy and Resolving Disputes Regarding the Client File* available at **www.cna.com/lawyersriskcontrol**.
15 *C.f.* Neb. Op. 2001-03 (2001); Mass. Op. 92-4 (1992); Ala. Op. 88-102 (1988); Ohio Op. 92-8 (1992); Colo. Op. 104 (1999); and Ky. Op. E-235 (1980).

Security Requirements: Data Security and Breach Response Obligations

Article 24 of the GDPR requires that data controllers implement "appropriate technical and organizational measures" to ensure adequate data security. It is important to understand that the GDPR is not a regulation that is technical in nature. It does not provide information technology recommendations as in ISO 27000.[16] Instead, the technical controls required by the GDPR focus on recognizing the latest technology available and balancing the use of those products with the reasonable cost of implementation given the type and nature of data stored by an organization (Art. 32).

Data Security

It is also not within the scope of this article to comment on proper information security practices for law firms. However, CNA has produced several publications on the subject.[17] At the present time, law firms are expected to be employing appropriate firewall and virus detection software, utilizing proper data encryption and secure communication practices, and actively training all firm staff on avoiding potential phishing attacks and other potential sources of malware. In other words, law firms should comply with applicable state rules of professional conduct relating to the competent use of technology in their practices[18], as well as maintaining confidentiality.[19] If a firm does not have the experience or expertise to develop and implement proper data security practices, the firm should seek the assistance of outside counsel or recognized vendor servicing the needs of law firms.

Breach Response Obligations

It is important for law firms to develop a breach response plan to mitigate potential damages in the event of a breach. The CNA publication, *Law Firm Data Breaches: A Legal Snapshot*, provides a broad overview of all of the various U.S. state data breach notification laws.[20] For law firms required to comply with the GDPR, the following additional obligations should be considered:

- **Definition of "Personal Data Breach":** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (Art. 4.12).
- **Consider Differences in Notice Requirements:** U.S. breach notification laws vary widely on the topic of what conditions require a breach to be reported. Some require notification if a third-party accesses a system, others require access plus exfiltration of data, and others require notification only if the data was not encrypted or whether there is a reasonable risk of harm analysis. The GDPR includes an analysis of the risk to rights and freedoms of the data subject, and does not include an exfiltration requirement.
- **To Whom Notification is Required:** The GDPR requires that an entity notify the proper EU Supervisory Authority[21] within 72 hours of becoming aware of a breach of personal data (where feasible) (Art. 33). In addition, the breached party must notify the data subject without undue delay (Art. 34).

16 International Standard Organization 27000 sets for the standards for Information Management Systems. It is typically considered the gold standard for data security processes together with the National Institute of Standards and Technology 800-1000.
17 For more information on cyber security recommendations please see *Safe and Secure: Cyber Security Practices for Law Firms and Caution in the Cumulus: Lawyers Professional & Ethical Risks and Obligations Using the "Cloud" in Their Practices* available at www.cna.com/lawyersriskcontrol
18 ABA Model Rule 1.1.
19 ABA Model Rule 1.6.
20 See *Law Firm Data Breaches: A Legal Snapshot* available at www.cna.com/lawyersriskcontrol
21 See GDPR Article 55 for the proper supervisory authority.

Final Thoughts

The GDPR represents a watershed moment in the recognition of personal rights to privacy and identity. Regardless of whether the GDPR applies to a domestic small or mid-size law firm, it provides an opportunity for all firms to engage in introspection into current data collection, processing and storage practices. If the extraterritorial scope of the GDPR applies to a particular domestic firm, it is incumbent upon the firm to acknowledge the additional effort it will need to undertake in order to comply. While it will take effort and likely the assistance of outside counsel or a proper vendor, it is not an insurmountable task. For U.S. domestic firms outside the scope of the GDPR, internal processes should still be reviewed and validated to ensure compliance with current standards. Bear in mind that simply because a law firm is not actively engaged in business within the EU, perhaps its clients do. So, regardless of whether a domestic firm may be the target of an enforcement action by EU authorities, clients may still demand U.S. firms to have many of the safeguards required by the GDPR.

This article was authored for the benefit of CNA by:
Michael Barrett

Michael Barrett is the Risk Control Director for CNA's Lawyers Professional Liability Program. In this role, he manages a team of highly qualified attorneys who are responsible for the design, content and distribution of risk control content relevant to the practice of law. He also collaborates with executive leadership from CNA's underwriting and clams teams to develop and execute strategies for profitable growth of the program. Prior to joining CNA, he was a successful defense litigator specializing in the defense of commercial and professional liability lawsuits. He is admitted to practice in Illinois and Pennsylvania and he is a Registered Patent Attorney with the United States Patent and Trademark Office.

Distributed By:

IOWA STATE BAR ASSOCIATION

CNA

800-679-7154 http://www.locktonrisk.com/iowabar/
Contact: Michael Schrandt mschrandt@locktonaffinity.com

The purpose of this guide is to provide information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the publication date. Accordingly, this guide should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA does not endorse any coverages, systems, processes or protocols addressed herein unless they are produced or created by CNA. Any references to non-CNA Web sites are provided solely for convenience, and CNA disclaims any responsibility with respect to such Web sites. To the extent this guide contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. In addition, any examples are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice. CNA is a registered trademark of CNA Financial Corporation. Copyright © 2018 CNA. All rights reserved. Published 9/2018