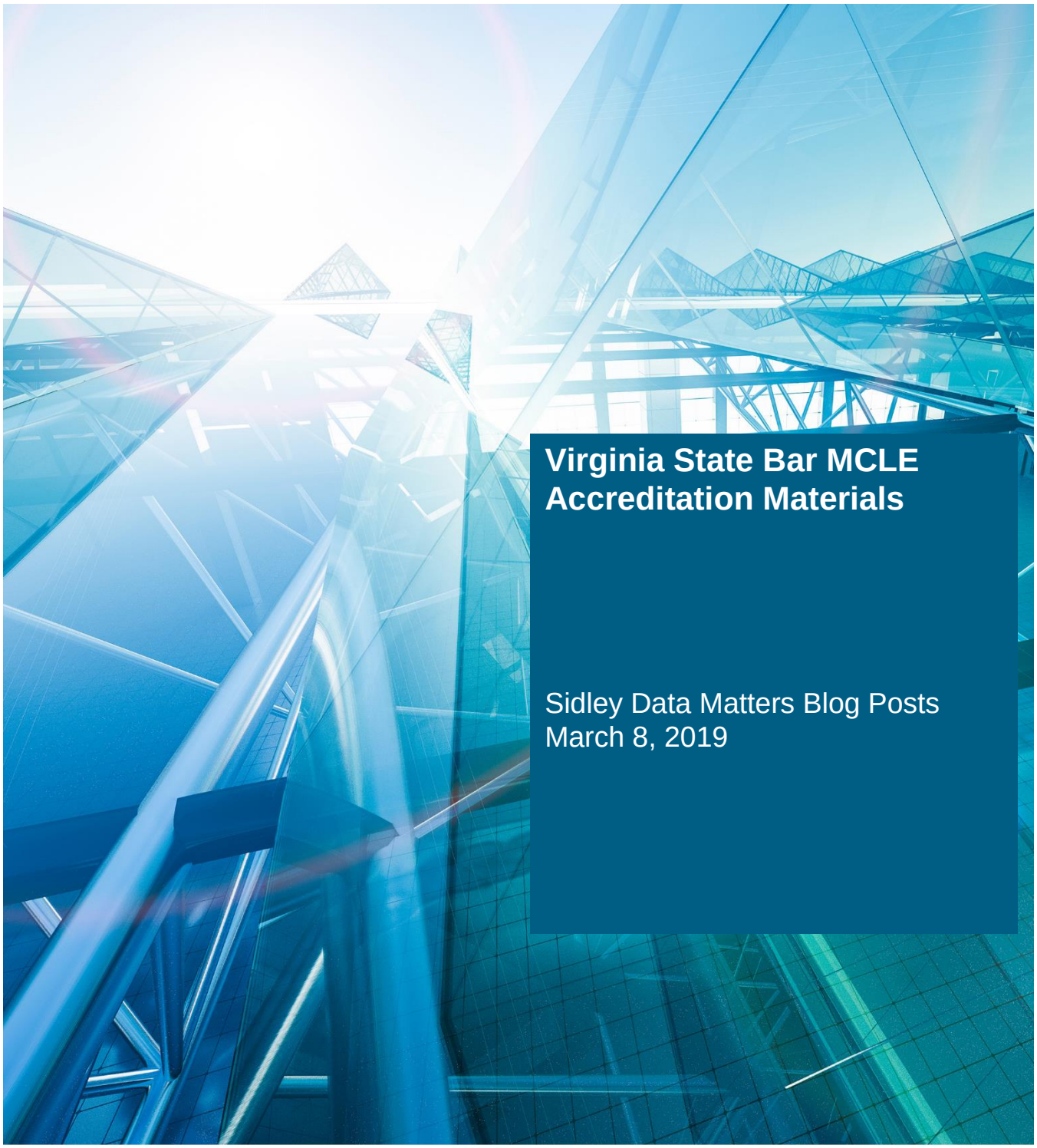

# Virginia State Bar MCLE Accreditation Materials

Sidley Data Matters Blog Posts
March 8, 2019

SIDLEY

TALENT. TEAMWORK. RESULTS.

# Table of Contents

# EUROPEAN DATA PROTECTION BOARD RELEASES STATEMENT ON THE REVISION OF THE ePRIVACY REGULATION

WIM NAUWELAERTS AND PAUL GREAVES

**May 30, 2018**

On 28 May 2018, the European Data Protection Board (the "**EDPB**") released a statement on the revision of the ePrivacy Regulation (the "**proposed Regulation**") and its impact on the protection of individuals in relation to the privacy and confidentiality of their communications. It is the first statement of substance by the EDPB since it was established by the EU General Data Protection Regulation on 25 May 2018. The statement calls on the European Commission, Parliament and Council to work together to ensure a swift adoption of the proposed Regulation, which will replace the current ePrivacy Directive (the "**Directive**").

The statement contains the EDPB's advice and clarifications on some issues which have been raised during the development of the proposed Regulation, which is still in draft form. Key messages from the statement include that:

1. **Confidentiality of electronic communications requires protection beyond what is offered by the GDPR**

The EDPB emphasizes the need for '*broad prohibitions, narrow exceptions, and the use of consent*' within the proposed Regulation.

The EDPB thus rejects suggestions that the proposed Regulation should permit processing of electronic communications content and metadata on what some may consider open-ended grounds, such as on the basis of the 'legitimate interests' of an organization.

The EDPB equally does not believe that organizations should be able to process electronic communications metadata based on the general purpose of the 'performance of a contract'. The statement notes that consent would not be required, on the other hand, to process electronic communications metadata which have been fully anonymized in accordance with EU guidance.

2. **The proposed Regulation maintains rights and obligations which exist today under the Directive**

In particular, the EDPB notes that:

- Transmission services used for the provision of machine to machine services are already in the scope of the current Directive; and
- The protection of terminal equipment is already a right (meaning that data controllers may only gain access to, or store information on subscribers' devices under certain conditions).
- The proposed Regulation maintains these rules, although it also includes new exceptions in areas where the EDPB considers there to be a limited privacy risk, such as in the context of security updates, and in the context of audience measurement.

3. **The proposed Regulation aims to ensure a uniform application across every Member State and every type of data controller**

The EDPB emphasizes that the changes are designed to ensure an equal playing field for all types of data controllers, in a technology neutral way. In particular:

- The proposed Regulation is aimed at bringing 'Over-the-Top' services within the scope of the rules, as the EDPB views these are functionally equivalent to traditional electronic communications services.

- The proposed Regulation's rules apply as soon as data relating to users' behavior are collected – whether or not users have created an account for a service.

- Service providers will need to obtain consent compliant with GDPR consent requirements. Notably, the requirement to obtain 'freely given' consent should prevent service providers from implementing so-called 'cookie walls' which block users from receiving the service if they do not provide their consent (in fact, the EDPB appears to support an explicit prohibition on 'cookie walls').

- Uniform application of the rules is achieved by aligning the sanctions and territorial scope of the proposed Regulation with those of the GDPR.

**4. The proposed Regulation must enforce the 'consent' requirement for cookies and similar technologies, and offer services providers technical tools which allow them to obtain that consent**

In particular, the EDPB supports the inclusion of provisions within the proposed Regulation which:

- Offer users control over the use of the storage capabilities of their terminal equipment;

- Require a 'privacy by default' approach in relation to software settings; and

- Permit web site and mobile applications to obtain users' consent through the use of privacy settings.

# FRENCH CNIL FINES GOOGLE €50M FOR VIOLATION OF GDPR'S TRANSPARENCY AND CONSENT REQUIREMENTS

WIM NAUWELAERTS, GERALDINE SCALI AND LAUREN CUYVERS

**January 24, 2019**

"On January 21, 2019, the French Supervisory Authority (the "*Commission Nationale de l'Informatique et des Libertés*" or "**CNIL**") issued Google's U.S. headquarters ("**Google**") with a fine of €50m for failure to comply with the EU General Data Protection Regulation's ("**GDPR**") fundamental principles of transparency and legitimacy. The CNIL found that the general structure of Google's privacy policy and terms & conditions was too complex for the average user and that Google, by using pre-ticked boxes as a consent mechanism, failed to establish a legal basis for data processing to deliver targeted advertising. This is the first regulatory fine the CNIL issued on the basis of the GDPR's penalty authorities, and it marks a strong enforcement signal to organizations subject to the CNIL's jurisdiction moving forward.

The administrative proceedings against Google were initiated through a collective claim filed with the CNIL on May 25 and 28, 2018 by two privacy rights organizations, NOYB ("None Of Your Business," founded by Max Schrems) and LQDN ("*La Quadrature du Net*"). The CNIL noted that LQDN in particular was mandated by more than 10,000 individuals to bring a complaint on their behalf. The NOYB and LQDN complaints urged the CNIL to investigate Google's data processing activities related to Android users who create a Google account (a prerequisite to use Google apps and services). The CNIL investigated the complaints and decided to commence administrative proceedings. The €50m fine comes only approximately 8 months after the claims were filed.

Google submitted an extensive procedural defense disputing the CNIL's competence to take action. Google argued that the data processing underlying the CNIL's decision, which covers a large number of Android users across Europe, contains a cross-border element and as such triggers the GDPR's cooperation and "one-stop-shop" procedure. The one-stop-shop principle is a preferential regime under the GDPR and submits organizations that are able to demonstrate centralized decision-making power to the enforcement powers of only one Supervisory Authority (the "lead Supervisory Authority"). According to Google, only the Irish Data Protection Commission, which is the authority overseeing Google's European headquarters in Ireland, could claim competence as lead Supervisory Authority as Google Ireland Limited is the main entity from a financial and commercial perspective (acting as counterparty in most commercial contracts with European clients) as well as the central Google entity in terms of resources and man-power (with over 3,600 employees). The CNIL, however, considered that these elements were insufficient to establish that Google Ireland Limited, at the time of the initiation of the investigation, had decision-making power with respect to the processing activities related to Android users. In particular, the CNIL pointed to the fact that Google Ireland Limited was not mentioned in the privacy notice as the decision-making entity for processing activities related to Android users, and that it did not develop the Android operating system (Google LLC did). Lastly, the CNIL noted that Google itself confirmed that it was in the process of "transferring responsibility" from Google LLC to Google Ireland Limited for the processing operations covered, and that this process would only be finalized by January 31, 2019. As such, the CNIL considered there to be no main establishment for purposes of the "one-stop-shop" regime, and asserted competence over the matter on the basis of sufficient territorial ties with France.

From a substantive perspective, the CNIL found that the information Google provides to its users on its data processing activities is not easily accessible, sufficiently clear and intelligible. In practice, Google's data processing activities are explained in different sets of documents (its privacy policy and general terms and conditions), and certain additional information is only available after having created a Google account or after the user has clicked on specific links in the documents (*e.g.*, "*to find out more, click here*"). The CNIL assessed that, in the case of targeted ad processing, five different user actions were required in order to access the full set of information that applies to the processing of the user's data. This approach was considered to lead to a fragmentation of valuable and extensive sets of information which were, according to the CNIL, already difficult for an average user to process.

Secondly, the CNIL found that Google's information notices were too generic, and in particular too generic in light of what they deemed to be the "intrusiveness" of the data processing activity at hand (profiling to deliver targeted advertising). Google's use of generic language was considered insufficient to fulfil the GDPR transparency requirement, which in essence should allow the user to clearly establish the scope of processing activities that involve his personal data.

The CNIL also used their finding that there was a lack of transparency to consider Google's legal basis for processing, user consent, to be illegitimate. The CNIL found that without sufficient information, the user is not able to take an informed decision as to whether or not to consent, rendering any given consent void. Moreover, the CNIL highlighted that Google's use of pre-ticked boxes as a consent mechanism could lead a user to consent to Google's targeted ad processing *by default*, which is in contradiction to the GDPR requirement that consent be "unambiguous" and expressed "by means of a clear affirmative action."

Given the particular nature of the processing involved and the specific position of the Android operating system on the French market (impacting millions of users), the CNIL's large penalty may not come as a significant surprise to many watching the evolution of data protection enforcement in the EU. However, the CNIL's critical findings with regard to information notices and consent mechanisms—emphasizing a need for notice and consents that are user-friendly, comprehensive and exhaustive at the same time—highlights a cumbersome, if not herculean, design challenge. This is especially true for organizations like Google which offer a wide set of applications and services driven by different processing operations and purposes and a variety of users. The CNIL's decision is now open for appeal before the French Council of State ("*Conseil d'Etat*") for a period of 4 months, and Google has already publicly stated that it will appeal the decision.

# EDPB ISSUES LONG-AWAITED GUIDANCE ON TERRITORIAL SCOPE OF THE GDPR

WIM NAUWELAERTS, WILLIAM RM LONG, CAMERON F. KERRY, COLLEEN THERESA BROWN, GERLADINE SCALI, LAUREN CUYVERS AND STEPHEN MCINERNY

**November 30, 2018**

On November 23, 2018, the European Data Protection Board ("EDPB") published draft guidelines seeking to clarify the territorial scope of the GDPR ("Guidelines"). The Guidelines have been eagerly awaited, particularly by controllers and processors outside of the EU looking for confirmation as to whether or not the EU data protection rules apply to them. The Guidelines largely reaffirm prior interpretations of the GDPR's territorial application under Article (3)(1), and offer essential guidance with respect to the GDPR's – heavily debated – extraterritorial application under Article (3)(2). The GDPR applies to companies established in the EU as well as companies outside of the EU that are "targeting" individuals in the EU (by offering them products or services) or monitoring their behavior (as far as that behavior takes place in the EU).

The proposed Guidelines are open for public consultation until January 18, 2019. It remains to be seen whether and how any outstanding issues will have been addressed upon conclusion of the consultation.

Some key takeaways include:

**Not all companies that process personal data relating to individuals in the EU are necessarily subject to the GDPR.** Where, for example, a controller in the EU designates a processor located outside the EU to perform processing activities, the processor will not be subject to the GDPR merely because it is exposed to personal data that originates from the EU. However, the processor will have to comply with certain contractual obligations that the controller is required to impose on the processor pursuant to Article 28 Similarly, a controller outside of the EU which processes personal data relating to individuals in the EU may fall outside the ambit of the GDPR if it does not "target" or monitor individuals in the EU.

**Companies outside the EU processing personal data relating to individuals in the EU may be subject to the GDPR** when they have an establishment in the EU and their processing activities outside of the EU can be considered "inextricably linked" to the (business) activities of that EU establishment.

**The application of the GDPR to processing activities must be assessed per controller/processor**. For instance, the designation of a processor in the EU by a controller outside of the EU for certain processing activities does not automatically bring both the controller and the processor in scope of the The processor is not considered an establishment of the controller for purposes of GDPR application. As such, the mere fact that the GDPR applies to, for example, a French subsidiary of a U.S.-based company acting as processor does not necessarily trigger application of the GDPR to the parent/controller in the U.S. In that case, the French processor will be subject to the GDPR's processor obligations only.

**Minor commercial presence on EU territory may suffice as an "establishment" for GDPR purposes.** One single sales agent or employee, operating through stable arrangements in the EU, may trigger application of the GDPR if the processing of EU-originating personal data is in the context of the activities of that establishment.

**The GDPR's extraterritorial reach only extends to the "targeting" or monitoring of individuals who are in the EU**. EU citizenship, residency or other type of legal status is therefore irrelevant to determine the scope of application of the GDPR. This would in theory also capture non-EU citizens whose behavior is monitored by an app whilst traveling in the EU.

**Indications that contribute to the targeting intention of service offerings to the EU market** are the launching of marketing campaigns directed at an EU audience, the inclusion of addresses or phone numbers in EU Member States, the use of a top-level domain name specific to an EU Member State, the inclusion of travel instructions to a country in the EU, but also the mere international nature of the commercial activity itself in some instances (e.g. certain tourist activities).

**"Monitoring" appears broader than foreseen in the GDPR's recitals**. According to the Guidelines, "monitoring" not only potentially covers online activity tracking via cookies, but could also include CCTV, Wi-Fi tracking and geo-localization activities. A case-by-case assessment needs to be performed in order to establish whether "monitoring" is performed.

**Controllers and processors in scope of the GDPR by virtue of Article 3(2) must appoint an EU representative via a written mandate**, such as a service agreement, and the EU representative can be a law firm, consultancy firm or an individual. In the opinion of the EDPB, EU representatives should not take on the role of Data Protection Officer for the same controller/processor. Data controllers should inform individuals about the identity of their EU representative at the time of data collection, e.g. in the privacy notice.

**The guidance leaves legal uncertainty for controllers and processor outside the EU on how to deal with the GDPR's data transfer restrictions (Chapter V)**. Controllers and processors outside the EU that find themselves subject to the GDPR are required to implement a GDPR compliance program, through which they offer an adequate level of protection to the personal data that are "imported" from the EU. Hence there are arguably no restricted data transfers in that case. Unlike recent UK ICO guidance, the Guidelines do not explicitly confirm that in such a case data transfer mechanisms are no longer required, and the EDPB did not address this question, leaving room for legal uncertainty. Hopefully this void will be addressed during the consultation round.

# EU DPAs RECEIVE THOUSANDS OF COMPLAINTS UNDER THE GDPR

WILLIAM LONG AND JASMINE AGYEKUM

**November 13, 2018**

European Digital Rights (EDRi), a digital user rights non-for-profit organisation, on 25 October 2018, launched an online platform, '*GDPR Today*'. In its first edition of the *GDPR Today*, the EDRi published statistics collected from eight EU Member States (France, Germany, Ireland, Italy, Poland, Romania, Sweden and the United Kingdom). The statistics show that since the GDPR's entry into force on 25 May 2018, data protection authorities (DPAs) have received thousands of complaints from EU individuals on the implementation of the GDPR by businesses and other organizations. Of note, the United Kingdom's DPA, the UK Information Commissioner's Office (ICO), has topped the list of complaints received, with nearly 15,000 complaints. Germany and France follow in the rankings, with 6,555 complaints and 3,767 complaints received, respectively. However, the UK figure includes complaints filed with the ICO prior to the GDPR's effective date.

The European Data Protection Board, the EU-wide independent data protection authority, has stated that more than 42,230 data protection complaints have been filed across Europe. However, the EDRi notes that as the GDPR grants EU citizens the authority to bring cases directly to the courts of Member States, this total figure may be even higher.

In relation to breach notifications, the UK's ICO has received 5,992 data breach notifications from businesses and other entities since 25 September 2018, far exceeding the 1,831 complaints and 1,308 complaints received by the Polish and Irish DPAs, respectively. The UK figure also includes data breach notifications filed under the previous UK Data Protection Act 1998.

It will be important to closely monitor whether and how this high volume of complaints translates into enforcement actions and trends in the coming months, as well as whether the insights that may be derived from such a volume of complaints may result in additional clarifying guidance from the EDPB or other data protection authorities.