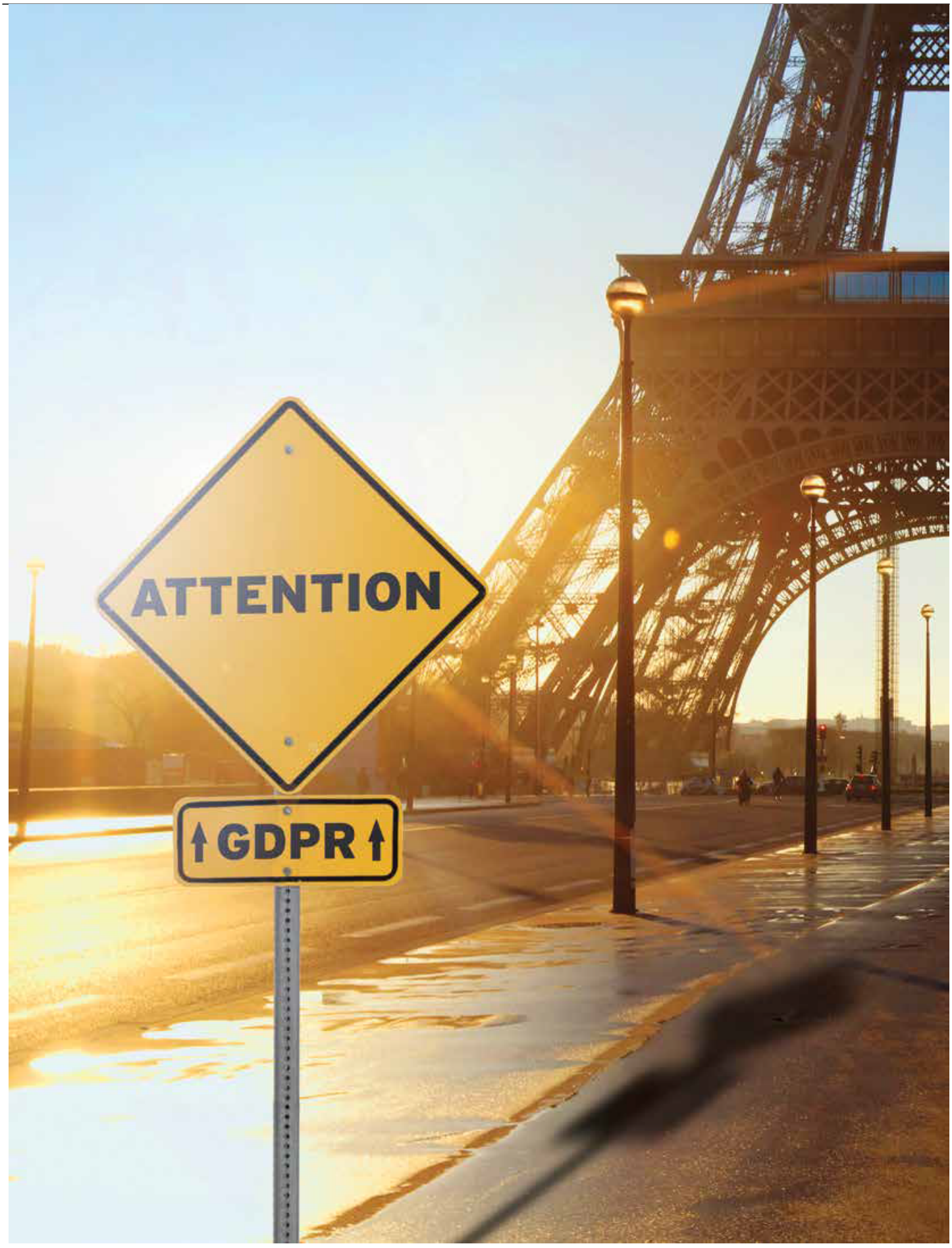
The Brave New World of Fines, Myths, and Reality: A French Regulator Perspective

Technology, Privacy, and eCommerce


ATTENTION
GDPR


ATTENTION
GDPR

CHEAT SHEET

- ***Questions left unanswered.*** Key European institutions agreed to formalize GDPR after nearly two years of debate, leaving many unanswered questions regarding the diligence of new sanctioning powers.
- ***Fear the DPA.*** France's data protection authority was significantly disjointed prior to the creation of the CNIL in 1978, which has since become a watchdog for personal data in the country.
- ***Inside the CNIL.*** The CNIL aims to work with a company's DPO in order to make it mutually beneficial to become compliant with new data regulations.
- ***Moving too fast.*** New regulations under GDPR are already becoming obsolete as the evolution of big data is outpacing the ability of legislators to foresee what needs to be done.

In January 2016, the law firm Baker & McKenzie brought together its European data protection experts for a roundtable in London on how to best prepare for the General Data Protection Regulation (GDPR), which had just been adopted by political consensus weeks before. A few clients were present, including the author who represented GE Capital — our company was still in fire drill mode from the Safe Harbor earthquake and had not yet given much consideration to the impending challenge that the GDPR presents.

The atmosphere was electric. "What is the single most important thing our clients need to know about the GDPR?" Brian Hengesbaugh, the practice group leader, asked his colleagues. Consent. Accountability. Processor liability. Data protection officer (DPO) requirements. The roundtable went round and round until Theo Ling, a partner based in Canada, declared "Sanctions!" Clients, including myself, nodded in agreement. We stopped there and discussion ensued. This is what put the GDPR on senior leaders' early warning briefings and compliance alert.

The Baker & McKenzie roundtable is the starting point of this article. It builds on the discussion in that crowded conference room, draws on first-hand experience from the sanctions department of the French Data Protection Authority (known as the *Commission nationale de l'informatique et des libertés* or CNIL) — as well as insider interviews — looks at technology challenges, and provides a personal glimpse into the workings of how one multinational organization, General Electric, prepares for dawn raids and adapts to data privacy risks. It's a brave new world indeed.

Looking back as a starting point

There was no lack of drama during the nearly two-year buildup for the GDPR's adoption. Existing data protection regulations were slowly gaining visibility as part of historical decisions such as the Google Spain case decided by the European Union Court of Justice (EUCJ) in May 2014, which secured a "right to be forgotten." Then there was the landmark Safe Harbor invalidation and Weltimmo decisions, which reinforced the reach of European data protection law to companies having an establishment in EU member states through "real and stable activities."

The most significant recent drama came in October when the EUCJ overturned the Safe Harbor

agreement, which had previously served as the legal basis for data transfers from the United States to the European Union and covered over 4,000 “self-certified” companies. The decision reached well beyond the international data transfers issue, also granting local data protection authorities (DPAs) more leeway to enforce local data privacy rules.

The European court handed the baton to the EU political apparatus at the end of 2015 as key European institutions finally agreed to the GDPR after nearly two years of debate. It was later cemented in April 2016 with the GDPR’s formal adoption and publication (officially in force after a two-year transition period, notwithstanding the possibility that EU member states may adopt certain measures before this deadline, which is already playing out in France).

There are still many questions left unresolved with the publication of the GDPR. Most significantly, how diligently will DPAs exercise their new sanctioning powers? From the corporate perspective, drawing on experience with GE, the key selling point to corporate leadership — which will generate more staffing requirements for privacy teams — has clearly been the risk of sanction and the reputational damage that would follow. There is uncertainty in how this will play out — and no shortage of anxiety and speculation as outsiders, as well as insiders, wonder how often DPAs will reach for the stick as opposed to the carrot.

In the beginning there were DPAs

The sanctioning question also goes hand-in-hand with the stated goal of harmonization. To what extent will DPAs be on the same sheet of music? There is good news in this regard. Article 79 of the GDPR will have a positive effect because presently there are significant disparities in terms of sanctioning power between the DPAs; each EU member state transposed the Data Protection Directive 95/46/EC (hereafter the Data Protection Directive) into national law according to its own tastes, and was able to effectively legislate well beyond the minimal requirements of the directive.

The eagerness of some DPAs to fine can be traced back in history, most notably in Spain, Germany, and France. These countries and others endured particular abuses during World War II. Their public psyche has since been wary of any form of personal data collection and processing, especially in regard to sensitive data such as religion. As Peter Hustinx, former European Data Protection Supervisor, recently commented, the focus on privacy and private life are relatively new concepts in Europe, “and an obvious reaction to what had happened in the Second World War.”

The creation of the CNIL illustrates this public concern. In the early 1970s the French government was on the verge of launching an ambitious project known as SAFARI with the goal of creating a centralized database on French citizens. This far-reaching initiative was intended to gather significant personal data, which would be collated according to the NIR (the equivalent of the national social security number). Public opinion quickly turned sour and the project was abandoned but the brief experiment did have one positive outcome (depending on one’s point of view): the 1978 adoption of the *Loi de l’informatique et des libertés* along with the creation of the CNIL. The CNIL has since been the watchdog for both public and private sectors in the domain of personal data and processing. Its powers have significantly increased in recent years and will continue to under the GDPR.

The Data Protection Directive was therefore not the starting point for data protection legislation in EU member states. The state of Hessen in Germany, for example, was the first to adopt data privacy legislation in 1970 (Sweden followed a few years later). The German system is particularly complex because it consists of one federal authority known as the *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, which came into existence with the federal data protection law BDSG

(*Bundesdatenschutzgesetz*). It was created in 1978 and included 16 federated state authorities (imagine, for example, an FTC-like government entity per state with significant political and administrative clout that enforces divergent and stricter standards).

Let them be fined… A look at Germany, Spain, the United Kingdom, and France

While the BDSG allows for fines of as much as €300,000, this amount is rarely imposed. Despite its restraint on the fining front, German DPAs have one of the strictest approaches to data protection. They were the first DPAs to impose mandatory DPOs in 1977. In addition, the German DPAs issued a position paper in the wake of the Safe Harbor decision, being the only DPAs to suspend all new approvals of Binding Corporate Rules (BCR). The state of Schleswig-Holstein has even gone as far as to question the use of model contractual clauses, as well as consent, for international data transfers to the United States. More recently, one German DPA issued the first fines for non-compliance with international data transfers following the Safe Harbor invalidation.

The case of Spain is unique. The AEPD (*Agencia Española de Protección de Datos*) was created in 1993 and is well known for its strict approach to enforcement through issuing fines. According to its 2014 activity report the AEPD issued 776 pecuniary sanctions and collected a record €17 million in fines. The AEPD's budget comes from fines as opposed to government coffers, which explains the eagerness of the Spanish DPA to fine.

One particularly draconian measure includes the AEPD's ability to issue fines for as much €600,000 for each infringement, resulting in significant collections for relatively minor cases of non-compliance. Google experienced this harsh reality first-hand in 2013 when it was fined nearly a million euros due to the non-compliance of its confidentiality terms.

In the business-friendly United Kingdom, the Data Protection Registrar was created in 1984, and replaced in 1998 by the Information Commissioner's Office (ICO) following the adoption of the Data Protection Act of 1998. It was not until 2010 that the ICO was given the power to fine organizations up to £500,000 for serious breaches, which did not prevent the ICO from teaming up with other regulators such as the then-Financial Services Authority (FSA) to issue more severe fines.

Generally speaking, however, the risk of fines is relatively moderate since non-compliance has to meet several specific conditions to qualify for sanctioning, including the number of data subjects affected, type of data concerned, and the behavior of the data controller. For 2014-2015, the amount of the 11 civil monetary penalties issued reached £692,500. In contrast, data privacy notifications fee income resulted in over £17 million. The shortfall will be problematic for the ICO since notifications will no longer be required under the GDPR.

The situation in France is yet another case apart. There are no fees collected for the mandatory data privacy filings that the CNIL requires (this paper shuffle will also come to an end under the GDPR, with the CNIL instead relying, like other DPAs, on the accountability principle for companies to keep their house in order). Fines are relatively modest, capped at 150,000 euros (or €300,000 for repeat offenders, which has never happened).

Google is a favorite target of the CNIL, having been fined three separate times. The first arose from Google's street view initiative — capturing personal details while failing to obscure faces — and resulted in a fine of €100,000 in 2011. The second case related to the company's failure to comply

with confidentiality terms, and resulted in another fine of €150,000 in January 2014. The third and better-known case, stemmed from the right to be forgotten issue and was levied in March 2016, costing the company €100,000.

While organization, structures, and philosophies vary by DPA, there does seem to be one common point hindering DPAs' bite. The amount of fines, in their current form, is relatively insignificant for large multinational coporations. Companies are, logically enough, more worried about trade control sanctions or antitrust issues than they are about privacy. Even the largest fines levied by DPAs, one of which was the fruition of coordination among six DPAs as well as a public warning from the Article 29 Working Party (WP29) aimed at Google's non-compliance with its street view and confidentiality terms, did not put a dent in Google's operations — or image.

The new regulation will change this. DPAs will have more clout and striking power to damage not only a noncompliant company's reputation, but to also hit its bottom line. The principle of *accountability* under the GDPR is key to this new reality. Firms, to some extent, will have to play the role of regulator — as Google learned following the right to be forgotten decision — and stay abreast of technology and understand the risks of its data collection and processing.

How it all works — inside the CNIL

The philosophy of the CNIL is unique and often misunderstood by American firms used to dealing with high-profile banking regulators or competition authorities. One of the CNIL's most important missions is to inform and counsel both the public and private sectors to raise awareness about risks and good practices to adopt. "The CNIL wants to work side-by-side with companies, helping them be compliant," remarked Karine Kiefer, the head of the CNIL Sanctions & Litigation Department.

The cornerstone of this approach, built around a genuine philosophy of pedagogy preached by the CNIL president, is built on its successful DPO network, which is effectively an extension of the CNIL's regulatory and compliance apparatus. Some 14,441 organizations have appointed a DPO, which is usually resourced internally from a company's legal, compliance, IT, or even HR department. The role is straightforward enough: Act as an internal watchdog to ensure that products and services are compliant with data protection rules.

In practice the DPO adds credibility to the organization and exempts it from certain formalities in terms of data privacy filings. But the DPO also suffers from problems of independence — inherent in being part of the organization itself — as well as seniority. "In many organizations in Europe the DPO is a little bit isolated," commented Winston Maxwell, a partner at Hogan Lovells. "There is not yet a process in place that gives the DPO real influence over the policies of the organization… companies don't yet recognize the importance of its function. It's a bit of a caricature but the DPO isn't somebody very important — he doesn't have a leadership role."

Designating a DPO in France was introduced in 2004 as optional, essentially a best practice nice-to-have. This will change under the GDPR since the DPO will become mandatory for the public and private sector in the event of large-scale data collection including profiling activities and when sensitive data is involved. Furthermore, the DPO will have more responsibilities, conducting risk assessments and analysis on data protection tools and issues. The person will also be the key intermediary with the CNIL.

Kiefer explains: "Today some DPOs are stuck, having flagged issues of non-conformity but the company takes no action. They call the CNIL and ask what they should do. With the GDPR, the DPO

is going to be the key intermediary with the CNIL as well as with other groups. This means that it will really be a workload in itself and not just an extra responsibility in addition to someone's day job." In the event of a visit by the CNIL, the DPO's role will not change. While most CNIL visits are unannounced beforehand, "Those who have designated a DPO are more likely to be informed," Kiefer commented.

In addition to BCRs — referred to as the "the virtuous path" by Winston because DPAs regard them so favorably — the CNIL offers other tools to encourage compliance. With the March 2014 French law "Hamon," the legislator introduced Privacy Seals — which are regulator-granted certificates for tools or programs that meet specific privacy standards — to companies, public authorities, or associations who have appointed a DPO. But in practice privacy seals have gotten off to a slow start given the formalities required to receive a "label" — requiring cumulative standards — as well as the limited number of categories where they are available: the internal organization of personal data management, the methods of verifying compliance with the law, and the handling of complaints and incidents.

Despite its vowed mission of pedagogy, the CNIL takes action when necessary. The CNIL's ability to sanction has gradually increased over the years. Since the adoption of the French data protection law in 1978, up through 2004, there were few onsite inspections. The law was updated after the Data Protection Directive implementation and visits increased significantly. The CNIL can now perform virtual online verifications of websites.

The CNIL's sanctioning prowess went through two significant modifications in the past 10 years. In addition to the legislative updates dating from 2004 cited above, the *Conseil d'Etat* — the highest government authority for advising the government or resolving disputes in public law — did its own sanctioning in 2009 for the CNIL's failure to adequately take into account the right of *responsables des lieux* (mandated company representatives) to refuse the CNIL's onsite verification. As a result the CNIL strengthened the rigor in its procedures and better documented its visits.

CNIL on-site visits increase every year. In 2015 the DPA conducted 510 verifications and 41 percent of those were at the initiative of the DPA — overall a 20 percent increase from the previous year. The verifications led to 93 injunctions (known as *mise en demeure*) — a procedure that requires a formal decision by the CNIL president — which technically does not qualify as a sanction since it falls just short, allowing organizations to comply by a certain deadline, which they do in most cases (or face formal sanctions).

While the *mise en demeure* can be viewed as a form of sanction by companies (since it's publicly disclosed and can have a reputational impact), the CNIL's stated intent is to inform the public of the compliance lapse and create awareness within the business industry. Such a decision, however, does not come lightly, requiring a special committee made up of the CNIL president and the two vice presidents. In 2015, for example, only 12 *mises en demeure* were publicly disclosed — relatively few, essentially lending more credence to the soft approach preferred by the CNIL.

One of the criteria the CNIL considers when adopting public disclosure is the type of organization it is dealing with (in additional to the overall behavior, proportionality, and the company's prior record). For example, the biggest CNIL fines targeted Google, and in 2015 there were only three monetary fines, two of which were made public for modest amounts.

Public disclosure of a CNIL's decision is a potent weapon. "In the end the most dissuasive method is not the amount of the fine. Public disclosure is the most feared," comments Kiefer. When the Google

fine was levied, the company went straight to the *Conseil d'Etat* to contest the public disclosure without paying much attention to the fine. But currently the risk of disclosure and fine are not necessarily tools that can effectively dissuade. Big international technology companies have not necessarily put data protection compliance on the topic of their business priorities.

The GDPR will change all of that. Article 83 of the GDPR will allow DPAs to fine companies up to four percent or two percent of the total worldwide annual turnover depending on the infringement and the conditions surrounding it, like the seriousness of the offense, the data sensitivity, the repetition, and the negligence criteria.

While the CNIL is familiar with the list of criteria for determining if a sanction should be levied, what will change for the CNIL is the notion of categorization for the type of sanction to apply (Article 83, °4 to °6 of the GDPR). But now the CNIL will also factor in an element familiar to those in competition and antitrust infringements: clemency. While clemency cannot be applied in the case of infringement, Article 83-k of the GDPR provides that the DPA can, when considering administrative sanctions, take into account "any other aggravating or mitigating factor applicable to the circumstances of the case…" This lends credence to the philosophy that it would make sense for the data controller to come clean with the DPA prior to the need for the regulator to come knocking. It gets more and more interesting as the story unfolds.

As illustrated above, one of the key focuses of the CNIL is on technology and information systems. The evolution of technology, and the reliance on firms to harness technological advances, will only underscore the need to stay abreast of data protection requirements and be on good terms with DPAs like the CNIL.

Keeping pace with technology

One of the underlying reasons for adopting the GDPR was that the current legal framework under the Data Protection Directive was no longer relevant given the technological changes of the past 20 years. It's a common argument that legislation is rarely capable of keeping pace with Silicon Valley. But in retrospect, the 1995 Data Protection Directive did surprisingly well when notions such as big data, cloud computing, and the internet of things were still years away.

In some ways the GDPR is already outdated. Technology advances have never lent well to such legal terms as *data controllers or data processors* — terms still very much present in the GDPR. Any experienced in-house counsel has surely spent time debating the question of which firm is *controller* and which is *processor* (only to come to the conclusion that both are controllers in various ways). And technology firms rarely have the time or the appetite to factor in the methodical and often laborious process of Privacy by Design or Privacy Impact Assessments; hence why companies like Facebook are so ill-equipped to take EU privacy requirements into account.

Take big data. Nebulous and often difficult to define, this idea refers to the ability of firms — either as *controllers or processors* — to harness vast amounts of data, including personal data, and process them for various business purposes such as targeted marketing, profiling for insurance risk analysis, underwriting, business analytics, or to develop new products or services. The uses are varied and the potential for abuse is very much a reality, including rendering seemingly anonymous data identifiable due to sheer mass of the collection. The GDPR tackles big data the best way it can, through accountability, which will be discussed in more detail below.

Cloud computing puts another snag in the legislative framework of the Data Protection Directive.

Crossborder transfers became unmanageable in the boundary-less space of the cloud, where data is stored on servers globally, processed with applications running on platforms hosted everywhere and serviced by IT professionals working remotely, from China to Canada to India. Try fitting a data transfer agreement into that paradigm. Or better yet try completing a data privacy filing to a DPA using a standard data transfer form like the one the CNIL requires.

The internet of things is yet another headache for data privacy professionals. The idea that objects are interconnected and data shared, usually in the cloud. Aircraft engine components that send back technical details of their performance, used to detect anomalies and plan for preventive maintenance. No harm there. But then take health data. Collecting health data or related personal data from at-risk patients and then transmitting this data to medical centers to monitor a patient's condition serves as an early warning for a potentially life-threatening emergency. The potential for good is indeed great — and no DPA wants to stand in the way of technologies that collect and process personal data for the benefit of public health. But how to define the limits? This is the challenge of the legislator as well as the regulator. Groups like WP29 — soon to become the European Data Protection Board under the GDPR — have been especially adept at providing guidance to these thorny questions.

Particularly interesting will be how European member states will implement provisions protecting health data since this is one area where they can diverge and adopt stricter measures. The question is on the mind of Lorraine Maisnier-Boché, in-house counsel to the government entity ASIP Santé (Agency for the Sharing of Health Information), charged with supporting the development of eHealth across France. ASIP Santé has the ambitious goal of creating the conditions for a trusted environment of eHealth, for instance by working on a harmonized legal and technical framework allowing health professionals to share medical information, through interoperable and secure information systems, as well as implementing eHealth information systems and managing certain eHealth records for the French government.

What's at stake in the eHealth arena is to reconcile the sharing of accurate data while respecting medical secrecy and a patient's rights," she notes. "To make this work, the development of software applications must embrace a privacy by design approach, and implement restricted access based on profiles while allowing the patient — for certain records such as the shared medical record, to mask certain medical data." No simple task. But there are already better practices out there, notably in Scandinavian countries, she observes.

Technology trends continue to outpace the ability of the legislator to foresee what will be the next big thing. The GDPR was drafted for this reality. DPAs' insistence on accountability as an underlying theme of what will change under the new legal framework is insightful. Isabelle Falque-Pierrotin, CNIL president and WP29 chairwoman, says, "First among these priorities is the accountability obligation. It's a new phenomenon in the European data protection law." She went on to add, "It's a key innovation in particular with the data protection officer."

But adopting accountability does not come overnight. Maxwell observes, "Because of the new sanctions regime, in terms of the data governance program, it takes time to implement accountability processes. Companies have to start now. Making sure that data protection is embedded in the organization when a new system using personal data is set up."

Two key elements of the new data protection framework hence lie not with the DPA or any specific innovation in legal doctrine, but instead with the need for companies to take responsibility for their innovations and the potential impact on data collection and processing. And the DPO, as an internal resource to the company, serves as a sort of outsourced regulatory supervisor within the company

itself, notwithstanding the shortcomings due to the lack of independence and seniority that often plagues DPO role.

GE experience — Dawn raids and beyond

In addition to GE's sophisticated compliance structure and shelves of policies and procedures to ensure that privacy requirements are taken into account and respected, the company conducts regular risk analysis to determine how to allocate resources and deal with any potential gaps. GE's recent adoption of its modified BCRs required a full-scale risk and gap analysis followed by tweaks to make the company's processes and organization consistent with its own internal code of conduct embodied by the BCRs. Given the complexity of GE's organization, it was a laborious and time-consuming process.

In parallel to the BCR drill, the company devoted considerable time preparing for an impromptu visit by regulators: the famed dawn raid. Dawn raid training has increasingly become part of the legal and compliance landscape at GE. While managing a regulator visit — be it from the CNIL or another regulatory authority — may seem intuitive and relatively straightforward, experience within GE has proven that it can be horribly complicated and high-risk.

Firstly, in the few cases experienced first-hand, key personnel are often not available when the regulator arrives. An HR manager or junior compliance officer may find herself face-to-face with a handful of experienced and determined government investigators, several of whom are touting large, yet empty suitcases and asking where the servers are kept. GE's hierarchical management structure does not lend itself to decisions being made locally without full coordination from more senior legal counsel, usually sitting in London or in the United States. When regulators are literally sitting in the conference room down the hall and have nearly finished their complimentary coffee there is no (more) time to stall.

A 2015 early morning visit by the AMF relating to the recent Alstom acquisition, occurred when the entire legal team was not available and the CEO was stuck in meetings at another location. The result: A human resource manager found herself face-to-face with the regulators and this author happened to stumble onto the group, eventually convincing them to return later and to a different GE site (needless to say, relieved to see the group leave the premises with empty suitcases).

Secondly, GE Capital, for example, is regulated by the US Federal Reserve, the Securities and Exchange Commission, as well as a host of country-specific regulators such as the Prudential Regulatory Authority (PRA), *Autorité des marchés financiers* (AMF), *Autorité de contrôle prudentiel et de résolution* (ACPR) … Not to mention the CNIL. Each of these regulators has a specific remit and understanding the potential risk to the company depends on which regulatory lens one uses, which may also differ by jurisdiction. Historically, data protection took a back seat on the risk matrix and the chief privacy officer did not have either the staffing nor clout to make much of a dent in priorities. The situation has evolved in recent years, however, due to high-profile data breaches, most notably within the healthcare business. The Safe Harbor invalidation and GDPR adoption are also starting to influence.

And lastly, overlapping responsibilities from legal to compliance and within business structures can result in the time-honored phenomena of *flight* or *punting* from high risk events such as dawn raids. When the crunch comes, senior and career-minded professionals can have the habit of deferring to more junior employees, essentially putting them in the hot seat, like pawns in a chess game, while circling from a safe distance and waiting for the right moment to swoop in and take charge. Since

responsibilities between the legal and compliance functions are not always clear, this phenomenon can be prevalent within an organization.

CNIL dawn raid — Real life case

This recent CNIL visit of a large company occurred without prior warning and required two days to complete — extending the time of CNIL visits has become more common due to the increasing scope of the CNIL's mission and time it takes to investigate a company's databases. The control began with the usual formality of informing the responsable des lieux (person representing the company during the visit) of the right to refuse the visit, followed by a brief presentation of the CNIL investigators and a company presentation including the business model and the database configuration.

The investigators set up in a conference room equipped with a video projector allowing the team to share information on the scope of the requests, essentially allowing all to take part in the discussions. The investigators conducted interviews with key personnel with a particular focus on database security and access. Interviews then gave way to real-time verifications to determine what personal data are collected and for how long, including how the data are collected and for what uses.

The investigators paid close attention to where the data are stored and any data transfers outside of the European Union. They also focused on how the company has implemented data subject rights to modify, oppose, or delete their personal data processing. To determine how this works in practice the investigators sit down with various employees across the company. They also take note of the computer room's security — with the responsable des lieux always present during these verifications. It's also possible that the CNIL investigators request to see the contracts in place with service providers managing personal data collection and processing.

Once the investigation is completed, CNIL investigators regrouped into a conference room provided by the company to draft their report (procès verbal or PV). The PV summarizes all the observations made during the day, noting all the various gaps observed but failing short of a bona fide sanctions list. The drafting is completed with extra diligence since the PV, along with additional documentation, could serve as the basis for a formal sanction.

Given the PV's importance, both for the investigators as well as for the company, the drafting lasted well into the evening. Once complete, the various stakeholders (involving firm lawyers, in-house counsel, IT specialists, etc.) carefully reviewed (and could request changes varying from small details such as the spelling of names or punctuation to more significant aspects such as the observations made by the investigators). The company also has the option to include its own observations as an amendment to PV — rare in practice — or can submit observations even after the PV has been signed.

The signing of the PV was the most stressful moment given the legal implications at stake, not to mention marking the end of a long day for both the investigators and the company's staff. Given the stakes of CNIL investigations — which will only become more significant now with the GDPR — the legal dimension is increasingly reinforced during CNIL visits, both by the CNIL as well as by company's legal team, which does not hesitate to call in external counsel for assistance.

Allocating resources to the right place

In terms of data protection, one of the more curious phenomena observed at GE was the tendency for the resources of an organization to migrate to low risk areas to the detriment of higher risk ones. This scenario played out to perfection within GE Healthcare, a business that by all measures, at least by virtue of its name, should have identified data privacy as a high risk area and staffed it appropriately. But instead there were literally no full-time legal or compliance resources dedicated to data privacy until a high profile data breach turned the business on its head.

Where did all the data privacy experts go? They were helping businesses where data collection and processing primarily involved corporate entities instead of individuals — and certainly no health data. As a case in point, GE Money, which processes high volumes of personal data as part of its credit card business, did not formally designate a DPO until the CNIL issued a formal warning for data protection lapses. Why take the risk of working in data protection in a business like healthcare or money when other low risk businesses offer the same thrill for less risk?

High profile and costly data breaches are sufficient wake-up calls to appropriately staff the organization with data privacy specialists. GE Healthcare now boasts a full team of privacy professionals while GE Capital's has waned in the face of the company's restructuring and refocus on its industrial businesses. The Safe Harbor invalidation also sent alarm bells ringing, as reminders from the CNIL and other regulators began to trickle in warning GE to update its legal mechanisms (primarily an issue for its suppliers due to the existence of GE's BCRs) for transferring personal data from Europe to the United States.

And the GDPR is the (sour) cherry on the cake, with the potential for up to a four percent fine of a company's global turnover — this equates to roughly US$5 billion for GE! While the reputational risk is indeed the bigger issue at play, such a colossal fine would nevertheless make shareholders flinch. This potential fine is what is elevating privacy professionals in the company to greater stature and creating a slow migratory effect of in-house counsel toward career opportunities in a field previously considered less promising. The brave new world thus offers unexpected opportunities.

Further Reading

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).

Commission Nationale de l'informatique et des libertés.

C-131/12 : Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

C-362/14 Maximillian Schrems v Data Protection Commissioner.

C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság.

Hustinx, Peter. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation" July 2013 European University Institute's Academy of

European Law.

Le Système automatisé pour les fichiers administratifs et le répertoire des individus.

The social security number in France, also called the numéro d'inscription au répertoire des personnes physiques (NIRPP or NIR), is a code that can identify someone according to gender, month of birth, department of birth, and registry number.

French law no 78-17 du 6 janvier 1978 modifiée le 6 août 2004.

The German Federal Data Protection Act (Bundesdatenschutzgesetz) (the "DPA") modified by the Federal Data Protection Act Amendment Law (Novelle des Bundesdatenschutzgesetzes), the majority of which entered into force on 1 September 2009.

Conference of German Data Protection Authorities Position Paper, 21 October 2015 S.

Positionspapier des ULD zum Safe-Harbor-Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14.

On 6 June 2016 the Hamburg Commissionner for Data Protection imposed fines on Adobe, Punica, and Unilever, in the amounts of 8,000, 9,000, and 11,000 Euro, respectively.

December 2013 : La AEPD sanciona a Google por vulnerar gravemente los derechos de los ciudadanos.

14 February 2007 FSA issues fine of nearly a million pounds to Nationwide Building Society pursuant to section 206 of the Financial Services and Markets Act 2000 (FSMA), in respect of a breach of Principle 3 of the FSA's Principles for Business which occurred between 1 December 2004 and 1 December 2006.

Internal Procedure for Issuing Monetary Penalty Notices, ICO website.

C-131/12 : Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

Article 37 of GDPR.

LOI n° 2014-344 du 17 mars 2014 relative à la consommation known as "Loi Hamon".

Another modification from the recent law 2014-344 expanding the types of controls that the CNIL can now perform.

6 November 2009, number 304300 and 3043001 in which the Conseil d'Etat cancelled two sanctions levied by the CNIL.

GDPR now imposes direct statutory obligations on processors and severe compliance for compliance shortcomings : See Articles 28 and 82 of GDPR.

Article 68 of GDPR.

Article 9.4 of GDPR.

Agence des systèmes d’information partagé de santé.

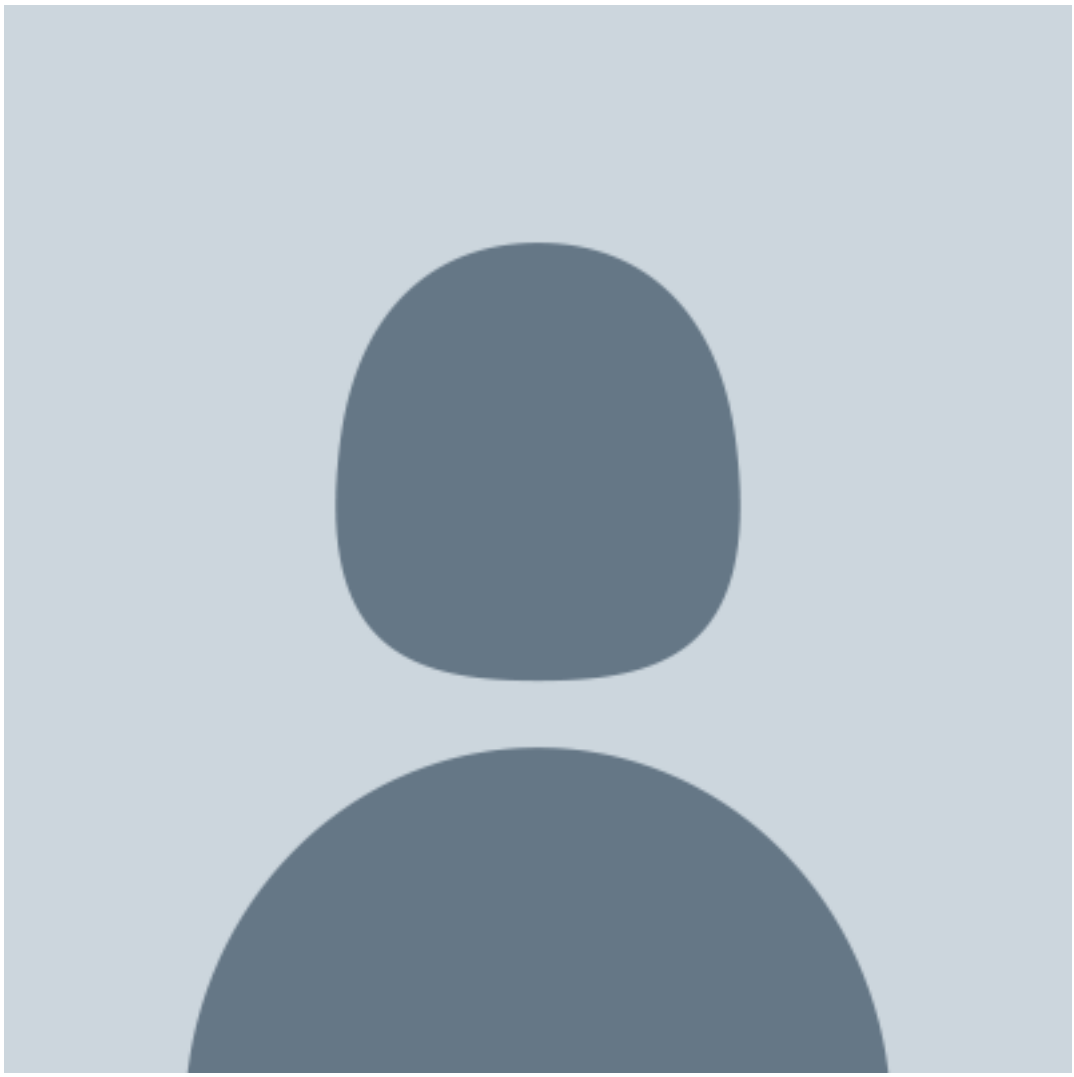
Comments made during the 2016 European Data Protection Conference held in Amsterdam.

Joseph Srouji

Avocat à la cour and Data Protection Officer

Joseph Srouji is avocat à la cour and data protection officer based in Paris, France.

Marie Veillon



Marie Veillon is a graduate law student at Université Paris II Panthéon-Assas and former intern at the Commission Nationale de l’Informatique et des Libertités (CNIL). marie