Privacy compliance challenges in 2020 and beyond

Marcelo Crespo, PhD, CCEP–I, and Guilherme Beloto

Marcelo Crespo (marcelocrespo@pgadvogados.com.br) is a lecturer, professor, and partner at PG Advogados in São Paulo, Brazil, where he performs legal services concerning digital law. Guilherme Beloto (guilhermebeloto@pgadvogados.com.br) is a political scientist and graduating law student currently involved with privacy and data protection projects at PG Advogados, assisting national and international companies based in Brazil.

- linkedin.com/in/marcelocrespoadv/
- twitter.com/professorcrespo
- linkedin.com/in/guibeloto/

Speaking of privacy compliance is much more difficult than it appears initially. From the complex regulatory scenario regarding personal data, to the incremental need for this same data for decision-making, this topic is a mix of such diverse subjects as governance, compliance, information security, user experience, and others.

Although it’s hard to determine exactly when privacy compliance became a hot topic, surely, since 2013 it came into the spotlight when Edward Snowden leaked details about PRISM, a surveillance program run by the National Security Agency (NSA) that had direct access to Google, Facebook, Apple, and other internet giants. British newspaper The Guardian and American newspaper The Washington Post revealed the information of the secret program in 2013, unleashing a chain reaction that would later change the public’s perception on data collection by government authorities and shaped the debate in the
following decade. The electronic eavesdropping of the PRISM program was part of a larger NSA system for massive data collection, sniffing data from a variety of individuals (targets), ranging from normal people to presidents. As information became public, we learned that PRISM allowed US intelligence to gain access from internet companies to a wide range of digital information on foreign individuals from outside the United States.

It was aimed to grow into a ubiquitous spying apparatus, able to monitor all the world’s citizens, and the fact that it wasn’t necessary to obtain individual authorizations from a judge to include someone as a target just made the program more dangerous for the privacy of individuals. Snowden’s revelation was scandalous, because PRISM didn’t need individual warrants. It was operating under a broad authorization from federal judges who oversee the use of the Foreign Intelligence Surveillance Act (FISA).

At that time, privacy compliance wasn’t subject to law, but it was a justified concern, considering people could have been spied on by the NSA. The revelation that PRISM allowed officials to access history, emails, file transfers, live chats, and documents made the world pay strict attention to it. For instance, Brazil seized the moment and passed its federal general law to regulate the internet, nº 12.965/14, which became known as Marco Civil da Internet (MCI) in a clear effort by the Brazilian government to demonstrate that there were laws regulating the digital environment. It was even rumored that President Rousseff had been targeted.

Since 2012, The European Parliament and the Council of Europe, in turn, were discussing the need to update their Data Protection Directive (95/46/EC) to face the new challenges arising from the development of the internet and the new technologies that allowed governments and companies to know so much about individuals. So, not long after, the General Data Protection Regulation (GDPR) came into force in 2018 and explicitly prescribed a global territorial scope, regulating what was already becoming a trend. The court case Google Spain and Google v. Agencia Española de Protección de Datos (CJEU C-131/12) broadened the territorial scope of the Directive, allowing the court to judge the global challenges being faced in this new context.

In Brazil, since 2018, there is a general law concerning personal data protection (known as LGPD, from the Brazilian Portuguese Lei Geral de Proteção de Dados). Although it is still in vacatio legis (adaptation period) until August
2020, it is already producing a cultural and organizational change in corporations, which are adjusting their methods to this new era of data protection.

Now, in the U.S., there’s a discussion of the relevance of having a general law concerning personal data protection, but no centralized federal legislation has been approved yet. The state of California has the most significant legislation of its kind, the California Consumer Privacy Act (CCPA), but even the CCPA is not as wide as other data protection legislation around the world, aiming at companies with “annual gross revenues in excess of twenty-five million dollars ($25,000,000), (possesses) personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers’ personal information.”[7]

It seems very clear that we are living in a significant moment that raises the bar concerning data protection. And it is happening around the world. To date, 107 countries have enacted data protection and privacy legislation,[8] and this number continues to grow, which demands companies’ awareness of privacy risks.

Regardless of which privacy laws affect your company, no doubt companies both in the online and offline worlds will have to pursue compliance, and there are some general challenges that may apply for all of them. Here we analyze the main challenges companies have when facing the troubled waters of a privacy compliance program.

**Challenge #1: Understanding the regulation as you pursue compliance**

It may seem very basic, but many companies do not quite understand what privacy laws effectively demand. Many still imagine that complying with the protection of personal data is more related to information security than proper good governance practices and protecting individuals’ privacy. That has led to totally distorted designs on projects. Many times, the consultant will be asked which tools must be bought and how their systems will handle privacy compliance. Of course, those are important parts of a privacy compliance program, but, first, it is mandatory to follow compliance pillars in order to
comply with good personal data governance. Tools will be helpful, systems may have to be adapted or even changed, but those are not the first things to be considered. In fact, they will be useless without tone from the top, a good risk assessment, and a deep understanding of the company’s corporate culture, for instance. Before hiring a privacy consultant, it is essential to understand what the regulation demands so you will be able to choose wisely for your consulting needs.

**Challenge #2: Choosing the best business privacy consultant**

Every time a new regulation comes into force, many consultants arise from dark places, naming themselves “the best specialist.” In the meantime, older consultants that never had anything to do with the subject start offering specialized services concerning the new regulation. And, of course, there are always those who have previously performed specialized services. This happens all the time, and it is no different with privacy legislation. It is undeniable that data privacy consultants know that privacy laws have generated great demand for their services, and so the industry has boomed overnight.

At this point, it must be said that there is no problem at all in seeing new consultants arise. The problem is that many times a “magical” solution is proposed that tries to simplify a complex reality, rendering itself incapable of covering significant risks that come out of new regulations.

This scenario makes it much more difficult for companies to choose who to partner with to help with the long-term road map of privacy compliance. After all, who should you have by your side? An information security expert? One that specializes in optimizing management? Law firms? Should you get tools for managing your privacy compliance program? And data loss prevention (DLP) tools? Although the need to respect privacy and protect personal data is not exactly new, it is still difficult for companies to understand the exact scope of their needs. Hereupon, choosing a good consultancy depends on many things, not only expertise from the consultant, but a broad menu of services to help you. Companies should have a good understanding of their governance maturity. After all, privacy compliance will demand some maturity. And last, but not least, it is important that consultants dedicated to your project
combine certifications, industry experience, and soft skills. There are lots of consultants with certifications, but they may not have practical industry experience or soft skills to deal with people from various fields (e.g., legal, IT, HR, compliance, auditing, user experience) and seniorities. In the complex network of interests involved in the program, a broad range of skills are necessary.

Challenge #3: Establishing the exact scope of the project

Because privacy laws are rules that encompass (to a greater or lesser extent) legal, governance, and technology aspects, it is critical to be very clear about the purpose of the project that your company will pursue. We have seen many cases that focused a lot on information security and left other aspects aside. A careful conversation with the client, explaining the aspects that will be dealt with and the limitations of what a consultancy company can do, can go a long way.

Establishing the exact scope of the project is as difficult as choosing the best business privacy consultant. It is very common for a company hiring a consultant to end up requesting other services not initially requested, and if the scope is not well defined, both the company and the consulting firm can have significant losses. The company loses because important aspects of risk may be left out of the project, and the consulting firm loses if the project is undersized in the initial planning and excessive work hours are required to carry out the project, which can be financially damaging, because more resources will be needed to complete it.

Challenge #4: Building a customizable global privacy compliance program

Being compliant to different local regulations can be very difficult once data is fluid and international in nature. Even if your company is not directly involved in some countries, it does not mean your company is exempt from complying with those privacy legislations, because there is a good chance you might be
processing data from there or your business falls within the scope of a foreign legislation. Let us focus our attention to GDPR. It covers the European Union (EU) and affects any business that deals with the data of EU citizens or people in the EU. So, even if you have a small amount of data belonging to any of the countries that are enforcing the GDPR, you could receive significant financial penalties and, consequently, reputational damages. It is not a risk worth taking.

In this perspective, it is even more difficult for a global company to comply. Once a company has businesses around the world, with business units located in many places, personal data flows are extremely complex. So, building a global privacy program is more than important—it is vital. It is not feasible to build country-specific privacy programs when there are a growing number of countries that have introduced comprehensive privacy regulations. There are points of contact between various legislations, with somewhat similar provisions in many of them, but the task at hand is to build a global program that can be customized to specific regions or country regulations (e.g., core features, supplemented by disclosures/sections for specific countries or regions). An in-depth program should fulfill the need for global guidelines with local customization. It is important, then, to identify common themes in privacy laws, such as privacy by design and privacy by default.

**Challenge #5: Building a program focused not only on protection**

It is also challenging to overcome the fear of punishment so that attention will also be turned to conformity for the sake of doing what is right, not just so that no monetary penalty is suffered, because focusing on the monetary penalties will hinder the full development of a compliance program.

Some consultancy companies also orient their program to avoid penalties, treating them as the only (or main) points of attention for compliance. In our view, this is far from ideal, because it fails to consider that a new scenario can also be a new business opportunity, either because compliance can bring reputational gains, or because it can even generate new products or services for businesses.

And, after all, great customer service and experiences keep people from causing problems for your business, especially those related to personal data.
You really should strongly consider revising the “heat” standards of complaints received. Bad key performance indicators should get extra attention. Improving an individual’s experience when interacting with your brand will keep you away from trouble.

Challenge #6: Consent

It has been widely said that the gold standard for the lawfulness of processing is consent. In fact, this is far from the truth, with both the GDPR and the LGPD providing for several other legal bases for processing personal data. Not only that, but consent is treacherous, and like a desert mirage, it can change in a split second, because it should be as easy for the data subject to revoke consent as it is to give it. This can create operational challenges, because there are important consequences for the systems handling the data. After all, how can we ensure the necessary agility to stop processing once consent has been revoked? Consent shouldn’t be used as a go-to legal basis for processing personal data, because there are other legal bases that can better stand the test of time.

Challenge #7: Never underestimate time while performing privacy compliance

Sometimes the challenge for a company is the time it takes to agree upon the adjustments of contracts or documentation (internal or external). Changes to business models are usually more difficult to undertake. Convincing the board and stakeholders can be a tough business, and there are no rules written in stone on how to conduct these changes.

Acquisition and system replacements can be quite time-consuming, and the learning curve can prove itself to be harder than predicted for some businesses and processes. It is important for companies to create a long-term program that can handle the unexpected, for there will certainly be unforeseen situations.

Conclusion
More than a hundred countries have laws concerning data protection. The main challenges, however, may not be the laws themselves, but how companies choose the consultants that will support them; how projects are measured and their scope; and how, in addition to escaping the fines, one can think of a global program that can be regionally customized and add value to the business. And this is much more related to knowing projects, the market, and business lines than necessarily the individual knowledge of one consultant. Adapting to new data protection regulations can further add value to companies, if done organically, by absorbing the principles that the standards bring about.

Probably not many will have this business view immediately, but we strongly believe this is a “plus” when privacy compliance is the job to get done. How does your company handle privacy challenges?

**Takeaways**

- Privacy is a new and complex concern regarding compliance matters, beyond surveillance.

- Privacy compliance is more than law and regulation adequacy; it is organic incorporation of privacy principles.

- Growing regulations around the world make global privacy compliance even more challenging.

- Global privacy compliance programs should be customized to specific regions.

- Consent should not be used as the main legal basis for processing, because it is too volatile for the stability of the business.

---


2 50 U.S.C. § 1801 et seq.


This publication is only available to members. To view all documents, please log in or become a member.

Become a Member Login