WHAT WILL COMPLIANCE WITH THE GDPR REALLY LOOK LIKE?

Sterling Miller
As we start to go deeper into 2018 there are a number of mysteries hanging out there on the minds of many good people: Does Bigfoot exist? Why is it called soccer? When will the next Game of Thrones book come out? And perhaps most importantly – what will compliance with the General Data Protection Regulation (GDPR) actually look like? As general counsel of a company that processes a good bit of personal data, I can tell you it is a question of high interest for my team and myself. As we are fast approaching the May 25, 2018, effective date of the GDPR, it’s probably a question on the minds of more and more in-house lawyers.

I’ve been involved with data privacy issues since the mid-1990s. I’ve met and dealt with many privacy regulators over the years and have been responsible for privacy compliance before the 1995 EU Privacy Directive was first published. Using this insight, I hope to share some ideas into what’s coming and what in-house legal departments should be doing to comply with the GDPR. Granted, none of us know how the various EU officials will actually enforce the dense text of the GDPR, but there are some things experience and common sense tell us we should focus on. To start, keep in mind the core principles of the GDPR:

- Lawful processing of personal data that’s fair and transparent
- Personal data is collected for a specific purpose and used only for that purpose
- Minimize the amount of personal data that is collected and retained
- Accuracy of personal data retained
- Security and confidentiality of personal data
- Access rights of the individual
- Accountability for all of the above

These are your guiding stars to GDPR compliance. Additionally, you need to understand whether you are a data Controller (the individual or company determining the purposes for and means of processing person data) or a data Processor (the individual or company processing data on behalf of a Controller), or both. Your obligations and exposure under the GDPR depend on your classification.

In my experience, regulators rarely act arbitrarily when enforcing a statute, especially one as new as the GDPR. Instead, what they generally want is proof you are working in good faith to comply and that you respect the process, including in your interactions with the regulators themselves. If you are deliberately not complying or you disrespect the process (and the regulators), your company can find itself in a mess of problems. Below are 10 suggestions on where companies should focus first to comply with the regulation:

1. **Place your bets**

   The first thing to understand is whether or not the GDPR covers your company. The question isn’t whether your company operates in the EU, the question is whether your company processes the personal data of an EU citizen. If you do so directly (Controller) or on behalf of another company (Processor), you are covered – no ifs, ands, or buts. If you’re not covered, you can stop reading here. For the rest of us, you need to place your bets. By this I mean, are you going to try to comply or are you going to ignore it or sit back and wait to see what happens? The latter is a strategy some companies are utilizing (both here in the U.S. and elsewhere), but this is a risky choice. First, if for some reason you fall under the regulator’s gaze, you will have absolutely no defense to claims you violated the law (and the fines can be quite high now, especially for those showing no effort to comply). Second, if you are a Processor, your customers must be asking whether you are GDPR compliant or not. If not, your business relationship may be shorter than you wish or you may start to struggle to get business. Third, if you are a publicly traded company and have not disclosed your lack of compliance, you can find yourself on the wrong end of a lawsuit if you get caught. If you are covered, make the effort to comply. Perfect compliance is not the standard, at least not by May 25. Good faith, substantial, and constantly improving compliance should be the goal coming out of the gate.
2. **Appoint a Data Protection Officer**

Under GDPR Article 37, if data processing is a core activity of your company, or your company processes a large amount of special category (e.g., sensitive) data, then you need to appoint a Data Protection Officer (“DPO”). Note, however, there is little guidance on what level of volume qualifies, so you need to decide where to draw the line. You can also voluntarily appoint a DPO if you want to demonstrate a positive attitude toward GDPR. If you process a good amount of personal data, you should appoint a DPO and not risk it. The DPO can be an outside party or an internal employee, but needs to be an expert on data protection laws and practices. The DPO is responsible for:

- Informing and advising the company on its GDPR obligations
- Being a point of contact for data protection authorities
- Advising on Data Privacy Impact Assessments (a process required under GDPR)
- Monitoring compliance with the GDPR (and other EU data protection laws)
- Ensuring compliance with the company’s data privacy/protection policies

You must ensure the DPO can operate independently, reports to senior management, receives appropriate resources to perform his/her job, and cannot be fired because he/she is doing their job.

3. **Train your employees**

Your Data Protection Officer is charged with ensuring compliance with the GDPR and your company’s data protection related policies. The best way to do this is by establishing a robust training program to ensure your company’s employees are aware of data protection and privacy issues. The most effective way to train employees (including senior management) is to establish a yearly privacy training course that must be completed and passed by all employees. This can easily be done online. There are lots of “out of the box” training modules and if they can be modified, you can increase comprehension by including data protection/privacy examples specific to your company’s business. Additionally, regular company-wide reminders from the DPO about the company’s policies and expectations are helpful. Finally, be sure to spend extra time (in person, if possible) with groups of employees working with data or in marketing as they are most likely to conceive of a use of personal data that may be problematic. If you train them to reach out to the DPO at the “idea stage,” you can avoid a lot of problems.

4. **Ensure data subject rights**

It is no secret that the most likely source of complaints to regulators about your company’s GDPR/data privacy compliance will likely come from individuals. GDPR Articles 12-23 create a number of new rights for the people whose data is being processed by your company, which means a lot more ways your company can slip up and find itself before a data protection authority. Nothing stops that data protection authority from widening its investigation of your company beyond the initial complaint by Mr. or Mrs. X. You goal, in part, is to stay off the radar. You will help your cause dramatically if you take the necessary step to ensure all of the GDPR data subject rights are made available:

- **Right to Access.** Data subjects (i.e., individuals) have the right to obtain confirmation from you whether you are processing their personal data, where it is being processed, and for what purpose.
- **Right to Correct Errors.** Data subjects can require that your company correct erroneous personal data without undue delay.
- **Right to Object.** Data subjects have an unfettered right to object to your company processing their personal data for purposes of direct marketing. If you receive such an objection, you must stop processing their data for that purpose.
- **Right to Be Forgotten.** This one is a real kick in the pants. Under GDPR, data subjects can demand you erase personal data about them. To do so, the data subject must withdraw their consent for you to process the data or the data has simply become outdated.
- **Data Portability.** The data subject is also entitled to receive from you – free of charge – their personal data in a “commonly used and machine-readable format” and be able to transfer that data to another company.
5. Transfer data properly

As you probably know, the EU is pretty proud of its data protection regime and how it protects the data rights of its citizens. So much so that it is illegal to transfer personal data out of the EU to any country that does not provide an adequate level of protection for that data. The United States – despite its myriad of sectorial data protection laws, but lacking a comprehensive data privacy regulation – does not satisfy the EU as providing an adequate level of protection. This means Controllers and Processors must have legal means to transfer personal data out of the EU to the U.S. (or to any other country not otherwise deemed adequate by the EU). Here are some of the ways to satisfy this requirement:

- **Explicit consent.** If the data subject gives explicit consent to transfer the data, then it is legal. Just be sure to keep copies of the consent.
- **Performance of a contract.** If the data needs to be transferred in order to perform a contract entered into by the data subject, then the data can be transferred. Note that if you want to rely on this exception, you must provide the minimum amount of data necessary to complete the transaction. For example, if an EU citizen orders something online from a U.S. company, they will need name, address, and credit card information. They probably don’t need birthday, age, etc.
- **Model Clauses.** The EU provides model contractual clauses for use by two contracting parties to permit the transfer of personal data. Read the clauses carefully before using them because they place a lot of burdens on the parties.
- **Binding Corporate Rules.** Under GDPR Article 47, these binding rules can legitimize the transfer of personal data between related entities. They need to be approved by the EU.
- **Privacy Shield.** This is a program agreed to by the U.S. and the EU in the wake of the collapse of “Safe Harbor.” U.S. companies can sign up to the Privacy Shield and, if the requirements are met, transfer personal data out of the EU. The requirements are stringent and there is an ongoing court challenge to Privacy Shield mirroring the challenge that brought down Safe Harbor.

6. Get consent

If you have an individual’s consent, you can do a lot of things with their personal data. But GDPR Article 7 makes obtaining consent more difficult than it was under the Privacy Directive. In order for consent to be valid, there must be a “statement or clear affirmative action” sufficient to demonstrate the consent was “freely given, specific, informed and unambiguous.” This means you can no longer rely on “opt out,” i.e., showing a box pre-ticked with an “X” and telling the individual they need to un-tick it to opt out. Instead, the individual must tick the box themselves. Equally important, the data subject must give specific consent for each data processing operation. If the processing operations are compatible, no additional consent is needed, but where that line is drawn is not clear. Additionally, there is a heightened requirement around consent for “special categories of personal data” such as health information. An individual can withdraw their consent at any time – in a manner as easy as it is to give it. Children under 16 (though Member States can lower the age to 13) cannot give consent, parental consent is required, and Controllers must make reasonable efforts to verify parents actually gave the consent. Finally, you should establish a process to track and document consent in case there is ever a dispute. If you cannot document the consent, it will be as if it was not given in the event of a dispute.

7. Update your privacy notice

Your website and the privacy notice contained on that website are your public-facing commitment to GDPR. This is the first place regulators will look when checking out your company. Don’t blow it. To properly update your privacy notice, your company must complete a Data Protection Impact Assessment in which you look deeply into what data your company processes and what it does with that data. Using that information, GDPR Articles 12-14 set out what is required in your privacy notice (and set out in easy-to-understand language):

- The identity and contact details of the Controller
- The identity and contact details of the data protection officer
- The purposes and legal basis for the processing
- Where the processing is based on legitimate interests, details of what these are
- The recipients or categories of recipients of the personal data
- Details of any transfer to a third country
- Details of the safeguards and the means by which to obtain a copy of them or where they have been made available
- The retention periods or the criteria used to determine that period
- Details on rights of access to and rectification/deletion of personal data
- Rights to object to processing and the right to data portability
- If processing is based on consent, the right to withdraw consent
- The right to lodge a complaint with the supervisory authority
- Details on whether the data subject is obliged to provide the personal data and the consequences of failure

Additionally, take advantage of this time and work on your privacy notice to ensure compliance with EU “cookie” laws as this is another area that can draw the attention of regulators if not handled properly.
8. Get Processor contracts right

It is becoming rarer that a Controller is also doing all of its own processing of personal data. More and more, such processing is outsourced to a third party, e.g., professional data processing companies located domestically or in third countries. The Processor can also be any third party touching the personal data – not just outsourcers. A Controller can allow a third party to process personal information on its behalf so long as all of the GDPR obligations on the Controller are passed along to the Processor pursuant to binding contracts, and the Controller does appropriate due diligence of the Processor. And if the Processor uses a third party (a “Sub-Processor”), it must pass its contractual obligations along via a binding contract as well. Additionally, the GDPR applies directly to Processors and makes them directly liable to data subjects. A big change from the prior regime. Under GDPR Article 28, specific contractual obligations must be passed down to Processors and any Sub-Processors, including:

- Process data only pursuant to instructions
- Ensure confidentiality
- Appoint a DPO
- Take all security measures required under GDPR
- Ensure any Sub-Processors contractually agree to same obligations
- Delete or return all personal data when the contract ends
- Be able to demonstrate compliance via documentation
- Help the Controller as necessary, including data breach notification and dealing with individuals request for their data

Interestingly, the Controller has the right to object in writing to any Sub-Processors, and the Processor has an obligation to inform the Controller of any Sub-Processors or any changes in Sub-Processors. One area in need of more clarity is when a Controller objects to a Sub-Processor. Is it a complaint to the EU, a lawsuit, termination of the contract? What if the Sub-Processor is GDPR compliant, SOC2 Type 2, etc. Is there a legitimate basis to object? The Processor/Sub-Processor relationship and ensuring proper contracts are in place between Controllers and Processors are likely to be high on the list of regulators. Getting these in place by May 25 is therefore critical.

9. Ensure “accountability”

If there is one area where the GDPR tightens up the responsibilities of Processors and Controllers, it is in the area of accountability, i.e., being able to objectively demonstrate compliance with obligations under the GDPR. In large part, ensuring your company meets the accountability standards will be the job of the Data Protection Officer. Moreover, compliance is more than just having policies, it’s being able to demonstrate that the company lives and breathes those policies. Fortunately, there is a proportionality standard in the GDPR, meaning that while your measures must be comprehensive, they can be proportionate to the size of your company and the nature of the personal data processed (again, where to draw that line is not clear). For Controllers, at a minimum, you need the following:

- Creation and use of Data Protection Impact Statements (DPIA) that analyze your processing of personal data and are used to minimize problems
- Recording of all personal data processing activities
- Appointing of a DPO (if required)

- Instituting and maintaining appropriate technical and organizational measures to protect personal data (such as password policies, limiting access to personal data to those who need to access it, data retention periods, etc.)
- Use of Privacy by Design standards to ensure that your company engineers data processing activities with privacy issues in mind from the start
- Ensuring that all Processors follow these same principles
10. Be ready for a data breach

You have probably heard the old adage that for any company it’s not a matter of whether there will be a data breach, it’s a matter of when. GDPR Article 33 takes this possibility head on and requires that Controllers (and Processors) be ready for a data breach. While hopefully it never happens to you, having a plan in place (that is practiced regularly) will go a long way in the event regulators ever come knocking on your door. In the case of a data breach (i.e., the loss of person information), Controllers have the following obligations:

- Notify the relevant national data protection supervisory authority within 72 hours of becoming aware of a breach. Notification is required, however, only if the breach would likely result in risk to the rights and freedoms of the data subjects:
  - Describe the nature of the breach, number of records, types/categories of individuals affected
  - Contact details for the DPO
  - An action plan for any remedial measures
  - Consequences arising from the breach
  - Documentation of the details of the data breach (to be provided when ready)

- If the data lost is “high risk” under GDPR Article 34, the Controller must notify the affected individuals “without undue delay” of:
  - The nature of the breach
  - The likely consequences of the breach
  - An action plan for any remedial measures
  - Steps the individual can take to minimize the impact of the breach to themselves

- Processors must notify their Controller within 72 hours of discovering a breach and must cooperate with the Controller in a manner sufficient to allow the Controller to comply with its obligations under the GDPR

It’s difficult to know exactly how the EU will enforce the GDPR starting May 25, 2018. It is unlikely that there will be hundreds of enforcement actions starting May 26. But you can be assured the EU and the supervisory authorities will be looking for the chance to make a statement about the seriousness of GDPR and the expectations for compliance. Not every company captured by GDPR will be 100 percent compliant on May 25. In fact, it make take several more months to inch closer to 100 percent compliance due to a myriad of factors, including waiting on further guidance from the Article 29 Working Party on just how to interpret and comply with some of the vagueness of the GDPR (so it’s worth monitoring their website for further guidance). But delay by regulators is not an excuse for non-compliance. I have identified above the areas where I think it is most likely the regulators will start looking for compliance. Nothing is certain, however, so you must look to comply in the manner best suited for your company. But, I do believe that if you can demonstrate good faith attempts to comply and you take the GDPR and the regulatory process seriously, the odds of a maximum fine under GDPR (or even any fine) are pretty low. Doing nothing, though, is not an option.

ABOUT THE AUTHOR

Sterling Miller has spent almost 25 years as in-house lawyer, including three stints as General Counsel. He is certified by the IAPP (CIPP/US). You can read his award-nominated blog, “Ten Things You Need to Know as In-House Counsel,” at www.TenThings.net and follow his regular posts on LinkedIn or Twitter @10ThingsLegal. His second book, Ten Things You Need to Know as In-House Counsel: Practical Advice and Successful Strategies, was published by the American Bar Association in 2017.