GDPR: THE NEXT CHAPTER IN DATA PROTECTION

By George S. Takach

Data protection law began in Europe a number of decades ago. So it is entirely appropriate that the next chapter in data protection law – the European Union’s General Data Protection Regulation (“GDPR”) – also comes from Europe. For Canadian organizations with operations or affiliates in the EU, GDPR will be important indeed. But to be caught by GDPR, one doesn’t have to have a branch or affiliate in Europe; it is enough that you have a virtual connection. That is, even if you do not have an “establishment” in the EU where personal data is collected or otherwise processed (which includes stored, used, or retrieved), you can be caught by the GDPR if you undertake any activity (such as offering goods or services to EU residents) that has a “real and effective” connection with the EU (even monitoring remotely the behaviour of EU citizens). And hence the importance of understanding some of the key new parameters of this broad sweeping data protection reform effort.

Why a New GDPR?

The EU legislation for GDPR was adopted in April 2016 by the European Parliament, and the new legislation comes into effect in May, 2018. As you will see from reading on, GDPR implements some novel concepts. But it also reaffirms some of privacy law’s longstanding core principles. Even these “fair information handling practices” (as expressed in the current EU data privacy Directive), however, were being implemented differently in specific countries within the EU, because each state in Europe was able to modify its relevant data protection legislation as it wished. This lead to inevitable inconsistencies across the EU.

This problem will be solved by GDPR, which for the first time will implement the self same legal privacy law regime across the full expanse of the 28 (to become 27 after Brexit) member countries of the EU. This will help organizations which have affiliates in several, most or all EU countries. That’s the good news. On the other hand, while the privacy standards to be met by organizations across the EU will be helpfully uniform for the first time, those standards themselves will be set higher.

Old Wine in Old Bottles

Many of the prior data handling principles of the soon to be replaced EU privacy Directive carry forward into GDPR. For instance, it is still a core principle that someone managing the data collection and handling process (typically in EU privacy parlance a “data controller” who oversees the relevant data handling practices, or a “data processor” who processes data on behalf of a data controller) adhere to a range of data processing principles, such as having to process data in a lawful manner (either pursuant to obtaining express consent, or because it is required for the delivery of a certain service).

Other such traditional data handling principles in the GDPR include: purpose limitation (processing data only for the purposes specified to the data subject); data minimisation (collecting only that data actually relevant to the approved function); data accuracy (ensuring the data is kept up to date and accurate, and allowing data subjects to require its rectification when it is stale or inaccurate); and data integrity (ensuring that data is stored in an appropriately secure environment). These various data protection principles have their analogues in Canada’s federal data privacy legislation (PIPEDA) and the various provincial counterparts. To that extent, they should be familiar to you.
New Wine, New Bottles

Now we turn, however, to the new provisions in GDPR. They are not just more of the same. They are net new, and some of them will prove to be very finicky indeed as they come to be implemented in the real world.

For example, it is now no longer enough to process data lawfully and fairly; under GDPR it must also be done in a transparent manner. This seems innocuous enough, until you begin to contemplate what this might mean (to allow data subjects to have the right to information regarding the data controller’s data processing practices). Consider you are a financial institution in Canada with an affiliate in Europe, and your Paris office has a complex new fintech methodology for approving personal loans. The system uses pathbreaking, novel artificial intelligence algorithms and work flows in order to make decisions as to whether to grant credit to individuals or not (say, students for their university education). The system also implements machine learning – that is, over time it compares its track record for loan repayment rates, and “improves” its credit granting decision making with each loan it approves or denies. In effect, it may well be that the bank, for any particular student applying for a loan, does not actually know how the system weighs the various personal characteristics and factual matrix of the individual loan applicant; or even if it did initially, the system “learns” over time, such that it never is stable enough to allow a human to understand the particular mix of variables that went into a certain decision. In such a case, how is the new “transparency” requirement of the GDPR to be met? What exactly do you tell the disgruntled loan applicant when they ask why they were refused credit?

The GDPR also includes a new data breach notification regime. Under GDPR, if there is a security breach, you must notify the relevant national data protection authority, and promptly (typically within 72 hours of learning of the breach). And if there is a potential harm to data subjects, they must also be notified. While these rules are broadly similar to those coming to Canada when the so-called “S-4” amendments to PIPEDA come into effect, the tighter timelines under the GDPR will require organizations to have even better data breach plans and procedures.

Another new and related requirement under the GDPR is that controllers and processors implement technical measures to ensure certain levels of security. In this regard, very important will be “pseudonymisation”, a new concept by which personal data can be “masked” or modified in a manner so that the data can no longer be attributed to a specific individual. This is an example of the GDPR requiring controllers and processors to undertake “privacy by design” when building their systems and workflows, so that the risk of data breach is reduced.

Enforcing Amnesia

Perhaps the data privacy protection rule garnering the most publicity in the GDPR is the “right to be forgotten”. In practice this requires an organization to erase personal information of a data subject under certain circumstances when asked to do so by a data subject. This can be demanded, for instance, if the data subject withdraws consent, or the information is no longer necessary for the original purpose for which it was collected.

These requirements are actually reflected (with some different language) in PIPEDA, so to that extent the principle is not that new in Canada. But here is what is different – if the data controller (essentially, the entity collecting the data) has made the data public (for instance, on a social media site), then that entity has an obligation to notify all others it gave the data to in
order to have them in turn erase the links to the data and so on down the chain of Internet random distribution. This will likely require organizations to create or adopt fairly elaborate computer systems in order to implement these legislative objectives.

The “right to be forgotten” raises some fascinating conceptual and practical questions. In short, our social media infused age, supercharged by the Internet generally, is creating untold of volumes of new data every day. One calculation suggests that more data has been created in the last 24 months than was brought into the world in all of recorded history prior to that time. In such an environment, implementing an effective right to be forgotten will be challenging for sure.

A similar (but easier to operationalize) new right that will invariably drive material IT development and deployment, is the new “data portability” right in the GDPR. For example, when an employee leaves one employer in the EU, and joins another, the data subject can require that the previous employer transfer his or her personal information to the new employer. Again, IT consultants will see material additional work from implementing this new requirement for data controllers and data processors.

**Non-Compliance is Not an Option**

The GDPR is very serious about compliance, as can be seen in the enhanced penalty regime instituted by the new system. A two tier approach is mandated. For certain transgressions (such as violation of the mandatory data breach notification), the fine is up to €10,000,000 or, in the case of companies, up to 2% of global sales in the prior year. This latter figure could be a very hefty amount indeed.

But wait – the total possible fine for a breach of: the right to be forgotten, consent requirements, and the right to object (among others) is set at up to €20,000,000 or 4% of global sales. These are some very significant thresholds for certain companies, and so expect the largest global companies – including some in Canada with meaningful affiliates in the EU – to amplify their global data protection legal compliance regimes.

Some commentators have taken the view over the past number of years that with the full on Internet, and e-commerce, and the unstoppable rise of digital generally in our lives, that privacy is dead and we should all just learn to live with this new fact of life. Well, clearly the law makers in Europe are not buying that line. Rather, in the GDPR, they are making a bold statement in the very opposite direction – that the principle of data privacy is important, and the legal system should buttress it. And with the size of the new potential penalties, even global tech giants will have to take heed of the privacy law gauntlet that is being thrown down in Europe.