COMPLIANCE WEEK
THE LEADING RESOURCE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

GDPR and the elevated role of compliance

The hefty compliance requirements of GDPR are going to require companies to figure out how to separate personal data from the ability to link that data to a specific person. Easier said than done, writes **Jaclyn Jaeger**.

The EU's General Data Protection Regulation is about to turn the compliance world on its head for all companies that collect or process personal data on EU citizens. Starting next year, everything companies historically have done with the oceans of data they amass and process each day will become illegal, absent new technical controls.

Since the early days of data protection, companies have relied on consent as the chief means of legally using an individual's personal data for the purposes of Big Data analytics, artificial intelligence, and machine learning. Through the convergence of these capabilities, computer algorithms analyze massive amounts of data, which companies use to make better and more informed business decisions. "The reality is that most businesses today are, in fact, data-driven," says Gary LaFever, CEO at Anonos, a GDPR compliance solutions provider.

Starting in May 2018, however, consent will no longer be a valid legal basis for processing data analytics. This is because the GDPR, while calling for individual control, heavily limits consent. "What the GDPR does for the first time is that it legally limits what an individual can agree to," LaFever says.

To process data analytics legally under the GDPR will require that consent be "freely given, specific, informed, and an unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her." This new, restricted definition of "consent" creates compliance risk, because once the personal data of EU citizens is re-processed for analytics, artificial intelligence, or machine-learning purposes and is combined with other data sets, it is not feasible for it to be described with specificity and unambiguity at the time of consent, LaFever says.

Moreover, the GDPR has no "grandfather" provision that allows for the continued use of data collected prior to May 25, 2018. Thus, all personal data a company has collected on individuals over the years—to the extent that it was reliant on broad-based consent—will be illegal.

The magnitude of GDPR penalties (up to 4% of global gross revenues plus joint liability among data controllers and data processors) make compliance an economic imperative.

Compliance vs. consent. Elizabeth Denham, U.K. Information Commissioner at the Information Commissioner's Office (ICO), has commented in public remarks that data protection is not simply about 'compliance.' Many companies today, she said, still have the mindset that, "'My job is to meet the legal requirements. As long as I tick the right boxes, we'll be okay.'"

That toxic mindset will not suffice under the GDPR. "[W]e need to move from a mindset of compliance to a mindset of commitment—commitment to managing data sensitively and ethically," Denham said.

That key point brings us back to data analytics: Once a compliance department signs off that it 'complies' with the GDPR, that does not then mean the company can continue to rely on consent for the processing of data analytics, or even continue to use historical databases, LaFever says.

This realization—that consent does not legally support data analytics—likely will come as a surprise to many companies, which are still only in the evaluation stage of analyzing their data and how it's being used. "A lot of people aren't fully ready for managing these issues," Hilary Wandall, general counsel and chief data governance officer at TrustArc (formerly TRUSTe), said in remarks at a recent GDPR Innovation Briefing in Europe.

Completing that initial evaluation phase is a "precursor to being able to effectively determine how they're going to control that data," Wandall added. Once companies wrap their arms around the data they have, that's when they'll really start to look at how to maximize the value of data within their organization and how to use it effectively to drive business strategy going forward, she said.

Compliance elevated. The GDPR effectively heightens the

role of chief ethics and compliance officers because, whereas privacy traditionally has been governed mostly by policy, it must now be technologically enforced, and in an ethical fashion. Compliance officers effectively become the business facilitators that enable growth.

Specifically, the GDPR provides a clear path forward by requiring that companies implement new technical controls—pseudonymization and data protection by default—to legally continue with data processing practices where consent will no longer suffice. "What those technical measures boil down to is granular control over the use of data," LaFever says.

> "The reality is that most businesses today are, in fact, data-driven."
>
> Gary LaFever, CEO, Anonos

Pseudonymization is a complex word, with a simple meaning: It requires that the information value of data be separated from the means of linking the data to an individual. "The application of pseudonymization to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations," the GDPR states.

The GDPR (Article 25) additionally imposes another new mandate, "data protection by default." This new technical measure requires that producers of new products, services, and applications consider data protection rights at the earliest stages of development. Traditionally, this has been the opposite approach, in which data has been available for use by default and then steps were required to protect it.

Article 25 states that, when data is available for use, provide access to only the data necessary to support each authorized use. "Basically, unprotect only those pieces you need, which requires that you can selectively and granularly protect those that you don't," LaFever says. "Pseudonymization is what you need to power data protection by default, because you need to be able to reveal just that level of information necessary."

Traditional privacy technologies—such as encryption, data masking, and privacy enhancing techniques—don't satisfy this new GDPR technical requirements for data analytics, because more data than is necessary is revealed for each authorized use. With enough identifiable information, traditional privacy technologies still make it possible to relink data back to the individual.

That's where a GDPR firm like Anonos can be of help. Anonos offers a "BigPrivacy" solution, for example, that enables companies to granularly control how they share data by controlling the linkability of identifying information to individual data subjects. At its core, controlled linkable data enables data to be used for a range of purposes while preserving privacy and protecting data from unauthorized processing and, thus, minimizing compliance risk and liability.

Legitimate interest. Although Big Data provides many benefits to a company, these benefits must be balanced against the fundamental rights of data subjects. That's where the concept of "legitimate interest" as a legal basis for using personally identifiable information without obtaining consent comes into play under the GDPR.

Article 6(1)(f) allows processing of data subject to a balancing test that weighs the legitimate interests of the controller—or third parties to whom the data are disclosed—against the interests or fundamental rights of the data subjects. What constitutes a "legitimate interest" requires careful assessment.

To this end, the Information Accountability Foundation (IAF) developed a comprehensive legitimate interest assessment process, published Sept. 10, which isolates important issues that need to be considered to ensure data processing appropriately strikes a balance between the legitimate interests of the data controller and the data subjects.

"One of the challenges of the GDPR is, while it introduces a risk-based approach and requires a 'balancing of the full range of rights and interests,' in the case of where risky processing is being undertaken, it is not particularly explanatory as to how this balance or assessment might be done or what factors should be considered," says Peter Cullen, executive strategist for policy innovation at the IAF. "The same is true of a legitimate interest assessment."

The IAF concluded that legitimate interest is most efficiently assessed as part of an integrated comprehensive data impact assessment (ICDIA), which it developed with input from business leaders and data protection authorities. "What an ICDIA does is it introduces a way to, in effect, perform an assessment to determine whether the benefits to an individual have been thought through and have the risks to an individual been effectively mitigated," Cullen says. "In short, it is a decision-making framework."

The IAF's work did not stop there, however. Through its work with stakeholders, the IAF said in its framework paper that it became clear that "the fact pattern that needed to be developed for the legitimate interest assessment was also the fact pattern necessary to determine whether a data protection impact assessment (DPIA) was necessary, and what the key risk and benefit issues would be for both as-

sessments." Therefore, IAF's scope changed from solely a legitimate interest assessment to, instead, legitimate interest as part of an integrated comprehensive assessment that includes a DPIA.

Marty Abrams, executive director and chief strategist at the IAF, says to assure processing is legal and appropriate, an organization must determine if a DPIA is necessary, "based on the level of risk associated with processing, what those risks might be, who is impacted by the risk, how the risks might be mitigated, whether there is residual risk, and, if using legitimate interests, the balancing of stakeholder interests."

The Article 29 Data Protection Working Party (WP29) cautions that the balancing test should be documented in such a way that it can be reviewed by data subjects, data authorities, or the courts. Thus, documenting the DPIA "creates a record if something goes wrong or the regulators want to do a spot inspection," Abrams says.

Given the extent to which data analytics is used by companies today, and the many business advantages it affords, not engaging in data analytics any longer may not be the best option. Nonetheless, the GDPR represents a fundamental change in how data must be processed moving forward.

Even companies that are not required to comply with the GDPR (those that do not process the personal data of EU citizens), implementing state-of-the-art technical controls like pseudonymization and data protection helps ensure that data processing for analytics, artificial intelligence, or machine-learning purposes is done in an ethical and compliant manner.

While the GDPR will require a fundamental shift in how data must be processed, it could also spark new and innovative ways to mitigate risk and gain customer trust, a win-win for compliance and business operations like. ■

GDPR ACTION STEPS

Below is an excerpt from a speech delivered by Elizabeth Denham, U.K. Information Commissioner at the Information Commissioner's Office, at a lecture for the Institute of Chartered Accountants in England and Wales in London in January.

The ICO's website has a twelve step plan to help organisations prepare for the GDPR. It sets out advice around making sure key decision makers know the law around personal information is changing, documenting the information the business holds, and reviewing privacy notices.

There's advice in there too around a few key areas of change in the GDPR, some of which may be relevant to your clients, such as dealing with subject access requests, consent for processing and handling children's data. It's only eleven pages, but by the end of tomorrow, it can leave you in a much better position to advise your clients.

Then next week, start getting a more detailed understanding of the new law. The ICO has just published an updated overview of the GDPR. It highlights the key themes of the new legislation, pointing to the similarities with the Data Protection Act, and explaining some of the new and different requirements.

There are sections in there on the principles the act is based on, the new rights enshrined for individuals, and also some detail on the derogations we might see, that allow for different countries to have subtly different laws. It will be a living document, with text added on different points as more guidance is produced, so familiarising yourself with it now, and reading the sections most relevant to your work, lays a solid foundation for offering advice around the law.

And next month, start taking the first steps towards understanding how GDPR expects businesses to put data protection accountability at the centre of their business processes. The overview has a useful section on accountability and governance, and will also point you in the direction of practical advice that should be useful to clients your advising.

I'd particularly recommend the code of practice for conducting privacy impact assessments. These assessments will have a key role to play under GDPR where organisations look at new ways of using people's personal data, particularly when that involves using new technologies.

Source: ICO