Three Game-Changing Impacts of the GDPR

Whitepaper | October 2017

As Published in

COMPLIANCE WEEK

THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Anonos®

THREE GAME-CHANGING IMPACTS OF THE GDPR

1) GLOBAL: If in the course of providing goods or services in the EU, your organization processes personal data of any individuals in the EU, the GDPR applies no matter where your organization is located.

2) ANALYTICS: EU residents can only legally consent to data uses that can be specifically and unambiguously explained at the time of consent. This significantly reduces the ability of organizations to rely on consent as a legal basis for iterative analytics, artificial intelligence and machine learning, since these activities cannot be explained with sufficient detail or clarity at the time of consent.

3) DATA ASSETS: Starting May 25, 2018, processing historical data is not lawful if records were collected using broad-based consent, which was the form of data collection most used before that date. The GDPR has no "grandfather provision" or "exemptions" allowing use of data collected without GDPR-compliant consent. **This creates liabilities requiring disclosure in financial statements due to potential lawsuits, regulatory fines and other actions, and lost access to data, all of which may harm operating results.**

The GDPR anticipates these issues and introduces new technical and organizational measures necessary to enable the data-driven economy.

The scope of the GDPR is now global, as opposed to prior EU privacy regulation that stopped at the boundaries of Europe. If your organization processes records of any individuals in the EU in order to provide goods or services in the EU, the GDPR applies no matter where your organization is located. The GDPR is more than a law pertaining to EU residents – it is the breaking wave of a tsunami of transformational data processing restrictions evolving around the globe. So, how do global organizations reconcile the growing importance of data analytics, artificial intelligence, and machine learning with the increasingly complex and multi-jurisdictional restrictions on lawful data use? The GDPR provides an answer in its requirement for new technical and organizational measures to protect personal data. Pseudonymisation, as defined under the GDPR, enables fine-grained, risk-managed, use case-specific controls to reallocate risk for inadequate data protection from individuals ("data subjects") to corporate data users. The importance couldn't be more significant.

Gartner predicts that by 2020, more than 40% of enterprise revenue will come from digital business. Similarly, IDC forecasts that by 2020, 50% of the Global 2000 will see a majority of their business come from their ability to create digitally-enhanced products, services, and experiences. **Yet the data-driven business operations that underlie these projections rely on data analytics, artificial intelligence and machine learning which are increasingly subject to restrictions on lawful data use such as contained in the GDPR and similar evolving regulations.**

Prior to the GDPR, the primary burden of risk for inadequate data protection in the EU was born principally by data subjects, due to limited recourse against organizations that collected and stored their data ("data controllers"), and lack of liability for data processors. However, this burden of risk is shifted by the GDPR's emphasis on rights of individual data subjects. As a result, a data subject's "consent" must be "freely given, specific, informed and an un-ambiguous indication of the data subject's agreement to the processing of personal data relating to him or her," to serve as lawful basis for processing personal data. These GDPR requirements are impossible to satisfy with respect to iterative data analytics, artificial intelligence and machine learning where successive analysis, correlations and computations cannot be described with required specificity and unambiguity at the time of consent. Additionally, the GDPR has no "grandfather provision" or "exemptions" allowing for continued use of historical data, as any data collected prior to the effective date of the GDPR would be using legally non-compliant consent.

To lawfully process data analytics, artificial intelligence and machine learning, and to legally use historical data, new technical measures that help support alternate (non-consent) GDPR-compliant legal bases are required. After May 25, 2018, companies that continue to rely on broad-based consent will not comply with GDPR requirements. Failure to comply with GDPR obligations exposes parties, including co-data controller and data processor partners, to fines equal to the greater of 20 Million Euros or 4% of global gross revenues of the ultimate parent company, plus additional significant obligations, liability, and exposure.

The good news is that Pseudonymisation, a new technical and organizational measure introduced under the GDPR, helps to support alternate (non-consent) legal bases necessary for iterative data analytics, artificial intelligence and machine learning, in addition to ongoing use of historical EU personal data.

The GDPR introduces a new concept of "Pseudonymisation" to support real-time, use case-specific, fine grain control over use of EU personal data. Pseudonymisation can help ensure that only the minimum data necessary for each authorized purpose is processed by "dialing-up" or "dialing-down" the linkability (or identifiability) of data to support legal data processing in compliance with GDPR requirements. This is simply game-changing.

Under the GDPR, Pseudonymisation is defined as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." GDPR compliant Pseudonymisation provides the following benefits:

- **Flexibility:** Support for GDPR compliant business operations requiring the linkability to, or the controlled re-identifiability of, individuals. GDPR Recital 29 speaks to selective access to data within an organization to ensure that people only have access to data as needed for their jobs and no more. Pseudonymisation enables an organization to retain their data, and share more of their data, by sharing or exposing only those discrete data elements needed for a specific purpose, and thereby support minimal necessary use.
- **Security:** Increased security controls help to reduce the likelihood and severity of data breaches and associated liability and negative publicity. Pseudonymisation applies "access controls" to the individual "data" level versus the traditional approach which applies to the individual "person" level. Pseudonymisation enables selective data access to control "what" each person can see and do at a fine-grained level, rather

than an individual's generalized access to an entire dataset. This approach reduces the risk of data loss, and reduces exposure, in the event of a data breach, to only the more efficiently protected data source at a fine-grained level, and not to the entire downstream interface or reporting outputs.

- **Compliance:** Pseudonymisation enables use of data to satisfy legitimate business objectives in compliance with GDPR requirements:

    - Alternate (non-consent) legal bases for data use: Reduces risk to data subjects in support of alternate (non-consent) legal bases for primary data uses [Art. 5(1)(a) / Art. 6(1)(b-e)];
    - Secondary data uses (further processing): Supports secondary uses (further processing) of data – such as Data Analytics – as a compatible purpose not requiring consent [Art. 5(1)(b) / Art. 6(4)];
    - Selective access to data: Enforces selective access to data within an organization and when data is shared between organizations to enable data minimization by limiting access to only that data which is relevant for each authorized purpose [Art. 5(1)(c)];
    - Archiving: Supports archiving of data for public interest, scientific, or historical research and statistical purposes [Art. 5(1)(e) – see also Art. 89(1)]; and
    - Enhanced security for data: Enforces granular technical and organizational measures to help protect against unauthorized or unlawful processing, accidental loss, destruction or damage [Art. 5(1)(f) / Art. 25].

	Enables GDPR Pseudonymization
Anonos® BigPrivacy®	✓
Security-Only Solutions (Encryption, hashing, static or stateless tokenization, data masking, etc.)	✗
Privacy-Only Solutions (K-anonymity, l-diversity, t-closeness, differential privacy, etc.)	✗

Shortcomings of Security-Only Solutions

A common approach to improving data protection is to prescribe security upgrades. The problem with relying on this strategy by itself is two-fold. First, security solutions limit access to data by enforcing generalized access/no access controls to entire datasets, preventing people without permission from accessing any data, or granting access, to all of the data. Security-only solutions do not support fine-grained, risk-managed, use case-specific controls over what people can do with data once they are granted access. Second, security technologies such as encryption, hashing, static or stateless tokenization, data masking, and related approaches, help to protect against unauthorized identification of data subjects using data that directly reveals the identity of a data subject, but do nothing to protect against unauthorized re-identification of data subjects by correlating data attributes to reveal identity via "linkage attacks."

Shortcomings of Privacy-Only Solutions

Prior to the GDPR, privacy was protected primarily using written contracts, "click-through" agreements and Terms of Service ("ToS") that set forth what organizations would be authorized to do, or not do, with data. However, for non-technical, non-preventive, policy-based measures to remain effective, controllers require resources and access to monitor compliance by the counterparties to contractual commitments. Such monitoring is typically unavailable or impractical to implement. Policy and contract based measures also place the risk from inadequate data protection on data subjects, due to limited recourse against data controllers and data processors for privacy violations. Technologies developed to safeguard privacy rights either work on a binary access/no access basis (e.g., data masking) or on an aggregated basis to support generalized statistics. In today's changing regulatory landscape, these technologies fail to comply with new GDPR standards for modern digital processing, or cannot support business needs for increased access to personal data without availability of consent. For example, combining and analyzing multiple data sets and incorporating unstructured data – processing which is at the core of the new digital economy – cause legacy privacy technologies to break down and prevent them from supporting GDPR compliant secondary data uses.

Benefits of Anonos® BigPrivacy®

Anonos BigPrivacy technology maximizes the value and usability of data by dynamically controlling the linkability (or identifiability) of data under controlled conditions at the data element level. BigPrivacy is a first-of-its-kind, patented platform that enables controlled re-linking (or re-identification) of data to retain and expand value after dynamically de-linking (or de-identifying) data to satisfy data protection, privacy, and security compliance requirements including, but not limited to, GDPR compliant Pseudonymisation.

The alternative to using Anonos BigPrivacy is increased liability and lost access to data.

Anonos has been actively engaged in research and development to advance the state of the art in data protection, privacy and security technology since 2012. The Anonos BigPrivacy systems, methods and devices that support GDPR compliant Pseudonymisation are covered by foundational granted patents (including, but not limited to, Nos. U.S. No. 9,631,481; 9,129,133; 9,087,216; 9,087,215; and 9,619,669) and a portfolio of over 50 pending U.S. and international patent applications.

The benefits of Anonos BigPrivacy enable global compliance controls on a jurisdictional basis necessary for secondary use (further processing) of data underlying the new global data-driven economy to unlock data value.

Contact Us

Contact us at BigPrivacy@anonos.com to learn about saving your data and enabling protected data use under the GDPR.

To learn how BigPrivacy technology is used in your industry, visit anonos.com/usecases

Anonos®

BigPrivacy® Unlocks Data

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