Forbes insights

DATA PROTECTION BY DESIGN:
The Opportunity In The Obligation Of GDPR Compliance

IN ASSOCIATION WITH:

pitney bowes

TABLE OF CONTENTS

INTRODUCTION

In recent years, some of the world's best-known brand names have found themselves sharing uncomfortable common ground with thousands of lesser-known counterparts—as targets of data breaches affecting hundreds of millions of people. The backlash to these and other major breaches has often centered on the careless and negligent attitude with which corporations are perceived to have guarded their customers' data—data that, in the wrong hands, can have a real and tangible impact on the lives of people affected. A large and well-known internet company, for example, came under fire in congressional hearings recently on a major breach involving 3 billion user accounts—a breach not fully discovered or disclosed until three years after it occurred. The tech giant's former CEO admitted to Congress that the company still doesn't fully know how the hackers accessed the accounts or how to fix the issue. Ultimately, the breach cost that company's shareholders $350 million, when—in the wake of the disclosure—it was acquired at a lower price than initially offered. In another example, a market-leading ride-sharing service admitted to paying a $100,000 ransom to the hackers of 57 million of its user and driver accounts in 2016. Countless other examples exist, with the common thread being compromised data that is exploited for unintended purposes.

While the General Data Protection Regulation (GDPR) is not a data breach regulation per se, breaches are a key focus. More broadly, the GDPR focuses on giving "data subjects"—the people whom the data describes—certain rights over how and when their information is handled or erased. This is really about consumer protection and the rights of individuals. In a sense, the GDPR signals a philosophical shift with regard to personal data, recognizing the safeguarding obligations that organizations take on when they collect or are entrusted with personal data. While this has been the EU perspective since the Data Protection Directive of 1995, which the GDPR supersedes, these are attitudes likely to spread considering the expansiveness of the law and the European Union's globally influential role.

Given that GDPR is designed to protect EU residents' data, regardless of where that data is collected, stored or processed, the regulation has wide applicability beyond the boundaries of the EU. That means many non-EU companies that have data on EU-based persons will be subject to GDPR and to its enforcement when it goes into effect on May 25, 2018. In turn, that means U.S. organizations, as well as those across Asia-Pacific and any other regions serving EU audiences (or with EU employees), will need to understand not only their risk of exposure under GDPR, but also how they can mitigate that risk through evolving best data protection practice.

Despite GDPR's broad enforceability, the consensus among industry experts is that businesses remain largely unprepared. While levels of preparation vary by industry and territory—businesses based in countries with already-strong consumer data protection laws, as in the EU, Australia and New Zealand, are generally better prepared—research data backs up general assertions on the lack of preparation. A 2016 business survey for Dell, for example, found that more than 80% of respondents, globally, knew little to no details about GDPR, and 97% had no plans in place to ready compliance.[1] In 2017, Capgemini Consulting surveyed banking and insurance firms and found them underprepared in terms of data privacy policies, breach detection and data erasure,[2] despite those industries already being heavily regulated.

Where there is awareness about the GDPR, it seems there is also a wait-and-see approach being taken and an unwillingness to invest in potentially unnecessary compliance measures. One reason may be that the path to GDPR compliance is not seen as sufficiently clear. "What has been missing is a clear list of tactical 'to-dos,'" explains Ilya Meyzin, vice president and data science chief of staff at Dun & Bradstreet. "Instead companies have had to rely on broad guidelines that can be interpreted in various ways and thus can also be misinterpreted." As a result, business leaders may have been wagering the uncertain cost of compliance against the cost of uncertain penalties down the

1 http://www.dell.com/learn/us/en/uscorp1/press-releases/2016-10-11-dell-survey-shows-organizations-lack-awareness
2 https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/privacy-and-cybersecurity-in-fs_dti-research-report.pdf

road. However, the release of several guideline documents by the Article 29 Working Party at the end of 2017 may go some way to mitigating this uncertainty. "From a non-lawyer perspective, some guidelines are quite detailed, with practical examples," explains Meyzin. "This extra clarity may help companies understand what the implementation entails and make decisions accordingly."

In any case, the EU has signaled it is serious about enforcing compliance in a way that, as outlined in Article 83, is "effective, proportionate and dissuasive." Guidance released in October outlined the approach that regulators should take to enforcement (see p. 7) and directs them to take into account the "nature, gravity and duration of the infringement," among other things, when assessing the response. There are several penalties and remedies specified, ranging from reprimands to data processing bans and financial penalties against both individuals and organizations. The harshest of these are fines of up to €20 million, or 4% of worldwide annual revenue, whichever is greater. That's certainly a large enough fine to get the attention of management. No organization wants to be the target of that sort of administrative action.

Regulatory action isn't the whole picture, however. The risks of losing customer confidence and the trust of industry partners in the event of a GDPR violation are very real—and may prove to be just as motivating as penalties. Besides the potential for lost business and canceled contracts, a slew of research has found that the reputational costs of regulatory sanctions far exceed the financial cost of penalties imposed. A 2010 University of Oxford research paper[3] and a 2016 analysis[4] from a progressive think tank, the Center for Economic and Policy Research (CEPR), for example, both found reputational damage and negative stock market reactions to regulatory action add up to somewhere around nine times the fine itself. If that pattern holds true with the highest tier of GDPR penalties, the effects could be devastating.

Risk of non-compliance aside, there are reasons GDPR compliance can itself be beneficial to an organization, whether in improving the quality of data, which in turn lays the foundations for deeper customer engagement efforts, or in improving customer confidence. This paper discusses some of those reasons—both the carrot and the stick—and, based on in-depth interviews with industry analysts, experts and data professionals, how a good approach to data can help speed compliance and tackle the obstacles to implementation.

3 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678028
4 http://voxeu.org/article/financial-market-wrongdoing-fines-vs-reputational-sanctions

DATA PROTECTION BY DESIGN: WHAT THE GDPR SAYS

With 99 articles and 173 recitals, the GDPR can seem daunting to tackle as a whole. Here we break down some of the key concepts and obligations under the law—with the caveat that this is not intended to be a comprehensive guide to the articles or the conditions under which they apply.

CONSENT: One of the most discussed bases for data collection and processing under GDPR is that organizations gain consent for doing so. Under this requirement, organizations must make it easy for individuals to give (or refuse) consent and make that consent easy to revoke. Consent must be obtained using plain language, avoiding "long illegible terms and conditions full of legalese." The regulation further states that data must be collected only for the purposes specified and not further processed "in a manner that is incompatible with those purposes." However, there are other conditions for collection specified under GDPR, and organizations should consider which is the most appropriate for their purposes.

DATA PORTABILITY: In certain circumstances, individuals also have the right to request that their data be transmitted, directly if possible, in a usable format to another organization.

DATA PROTECTION BY DESIGN: Outlined in Article 25, "data protection by design and by default" is perhaps the closest thing to an overarching theme of the GDPR. It says data protection should be central in the design of data processing practices. This includes implementing data minimization and integrating the "necessary safeguards" to protect the rights of data subjects. Recital 39 gives further light to the overarching tone: "Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed."

EXTRATERRITORIAL SCOPE AND PENALTIES: The regulation applies to most companies processing personal data of those residing in the EU, regardless of where the processing is performed, so the GDPR is also intended to subject non-EU organizations to enforcement.

RIGHT TO ACCESS/CORRECTION/ERASURE: Upon request by an individual, in most cases organizations must deliver the personal data held on a person, including the purpose it was held for, and at no cost. An individual also has a right to correct the record, and—when certain conditions are met, including that there are no "overriding legitimate grounds" to retain the data—the right to have that data erased.

SELECTED TERMS

DATA PROCESSING: Includes any actions taken with personal data, automated or otherwise, including collection, organization, storage, alteration, retrieval, use and dissemination (among other actions).

DATA SUBJECT: An "identifiable, natural person." A distinction: While GDPR applies to personal data about individuals—including sole proprietors of businesses—it does not apply to business data related to corporate entities. Businesses should ensure they are well informed on which data is subject to GDPR.

LEGITIMATE INTEREST: The GDPR states that there must be a "legitimate interest" in processing data. The U.K.'s

Information Commissioner's Office (ICO) elaborates that these can be a business' own interests or those of a third party, but they must be necessary and should not be able to be reasonably achieved in another, less intrusive way.[5]

PERSONAL DATA: Defined in the regulation to broadly include "any information relating to an identified or identifiable natural person," taking into account "all of the means reasonably likely to be used" in identifying that person. Although still considered to be personal data, "pseudonymized" data cannot be used to identify a person without the addition of other, separately held, data, and so its use is encouraged to mitigate risk.

EFFECTIVE, PROPORTIONATE AND DISSUASIVE: GDPR PENALTIES

In October 2017, the EU released its guidance for regulators in assessing violations of the GDPR, giving businesses their first insight into the thinking enforcers will apply in deciding penalties—and perhaps also impetus to take action. One of the overriding principles outlined in the GDPR is that penalties should be "effective, proportionate and dissuasive."

While it won't be clear exactly how aggressively enforcement will be pursued until the first penalties are handed down, the guidance does give clues. Regulators have a lot of discretion in how to act. They are instructed to take into account the "nature, gravity, and duration of the infringement,"[6] mitigating actions taken by the organization, "intentional or negligent character of the infringement," the technical and corrective measures taken and appropriate levels of security, among other factors. A defensible position will therefore likely take into account progress toward compliance and genuine efforts to mitigate harm, along with documentation to support those efforts—meaning the sooner compliance efforts start in earnest, the better.

TWO TIERS OF FINES

Article 83 outlines the conditions under which fines can be imposed, and two tiers of violation:

Up to **€10 MILLION** *OR* **2%** of total worldwide annual turnover, whichever is greater.

For violations including: failure to report breaches to the data processing authority (DPA) or to the individual concerned (data subject); failure to appoint a data protection officer (DPO).

Up to **€20 MILLION** *OR* **4%** of total worldwide annual turnover, whichever is greater.

For violations including: consent breaches; non-compliance with data access, correction, erasure and portability rules; and illegal transfers of personal data to non-compliant EU countries or organizations.

Regardless of any outstanding uncertainty around the penalty framework, regulators have made it clear they are serious about enforcing GDPR's provisions. Public comment on the October guidance closed in January 2018; further clarification from both EU and national regulators is expected.

5 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/
6 https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

DISCOVER, PREPARE, ACT: STEPS TO DATA COMPLIANCE

GDPR compliance is not possible without quality data, data management practices and the advanced capabilities to curate it. Many of those capabilities do not exist today within organizations because of internal gaps in technical infrastructure or processes. Compliance touches on multiple areas within a business—legal, IT and marketing are all important stakeholders—so multiple groups need to come together to ensure success.

Practically, organizations need to be able to quickly query and return all relevant information on individuals; allow individuals to correct, move and remove data relating to them; and, in the event of a breach, notify regulators. In situations of "high risk," organizations may also need to notify affected individuals. Carrying out these actions requires the ability to create a single, unified record for each data subject. "That doesn't mean it has to be all in one system," says Chris Butlin, director, professional services customer information management, Pitney Bowes. "The unified record can come from a number of different systems and be stored as a referential metadata object. But it should be consistent across those systems." Acquiring the ability to produce such a unified record is non-trivial and—depending on the age of an organization's infrastructure—can be very costly.

There are a few common stumbling blocks for organizations when tackling this set of requirements for the first time.

- **KNOWING THE PROCESS:** "The biggest initial obstacle is just knowing what data you've got and where you've got it," says Butlin. Overcoming this challenge can be straightforward when the data in question is static (i.e., it doesn't change once captured) and limited to structured databases such as those in customer relationship management (CRM) or enterprise resource planning (ERP) software. But it gets more complicated with unstructured and dynamic data that changes continuously (e.g., a person's location). These kinds of data exist in everything from text box comments to social media feeds and Excel spreadsheets, and all may hold vast amounts of customer data. "And that's probably the data that's potentially highest risk," says Butlin.

- **KNOWING THE DATA:** There are often multiple versions of the same data. According to data journalism website fivethirtyeight.com, for example, more than 31,000 people in America share the name James Smith, making it the country's most common name.[7] This multiplicity would present a major problem under GDPR because an organization needs to be able to differentiate between James Smith from, for example, London, England, where the name is also common, and a James Smith from Londonderry, Northern Ireland. Various name abbreviations, spellings, misspellings—accidental and deliberate—complicate things further. J. Smith and J.S. Smith may be the same person, and while Jim Smith consents to marketing emails, Jimmy Smith does not. So, when a James Smith requests his data, or a correction to it, the organization needs to be absolutely sure it's pulling all the right and relevant records. "And that's one of the tricks in this process," says Andy Berry, vice president, EMEA, at Pitney Bowes Software. "It's not just being able to pull one record, it's understanding that you might have the same person replicated across your system in many different name interactions, addresses, phone numbers."

- **KNOWING WHOM TO INVOLVE:** GDPR isn't purely a security or IT issue, it's a larger, more pervasive business issue. Planning for it should involve multiple stakeholders. All too often, marketing isn't even brought into GDPR discussions, yet that's one of the primary areas where this information is collected or derived. It's unlikely that all the knowledge required for compliance already exists in-house, so bringing in outside help and hiring the resources where needed should also be top considerations.

7 https://fivethirtyeight.com/features/more-evidence-james-smith-is-the-most-common-name-in-the-u-s/

Daunting though the task of compliance might seem at the outset, organizations may find that only a few of the 99 articles require specific action plans. Ray Umerley, vice president and chief data protection officer at Pitney Bowes, has been involved with the company's own process to comply with GDPR. He says the task becomes much more manageable once organizations can ascertain which specific articles apply. "But again, you have to get a handle on that early," he says. "We were able to distill our significant areas of change to maybe five or six groups of articles—and even then, it was things we already had a process for, but we needed to modify or expand upon."

The steps involved in a data quality approach to GDPR can be broken down into four main areas.

1. **DISCOVERY.** Before GDPR compliance can be achieved, data needs to be catalogued to record what data is stored, where and why; whether it's structured or unstructured, and whether it's stored digitally or in analog form. This is more a consultative exercise than an IT process. Berry explains: "It's trying to understand how much data, how many silos, how many legacy systems, how many marketing databases—it really is just an audit process across the operation."

2. **PREPARATION.** Data minimization is central to many of the requirements of GDPR, so decisions will need to be made around what personal data is necessary to have, under what basis it is being collected and what can be deleted. At the same time, the quality of the remaining data will need to be improved: Duplicates must be found and resolved, and conflicting data must be validated against credible sources to ensure accuracy.

3. **ACTION.** This phase requires a system that enables the data to be queried and subsequently delivered, deleted, corrected or ported when it is requested. "The art is, how do you access that data in real time?" says Berry. "So that when a consumer walks through the door and says, 'What do you hold on me?'—you can go through your network and gather all that information."

4. **GOVERNANCE.** Establishing the right governance model out of the gate is absolutely critical.There should be an internal body not only with the authority to orchestrate the above phases but also with the remit to change processes and oversee their implementation. Part of this process may be designating the data protection officer, as outlined in the GDPR itself.

"Essentially, you're going to have to make sure that you understand the data you have, and document why you're processing that data and handling that data—and to be able to show that on demand," Umerley summarizes. "I think that's something that a lot of organizations are going to have to look at doing sooner rather than later, if they haven't already started."

A NON-DISRUPTIVE APPROACH

Businesses will be looking for a compliance approach that deals with the sheer volume of accumulated data quickly and with as little disruption to business-as-usual as possible. In the narrow sense of a strategy that allows organizations to surface and manage those single, unified records outlined in the previous section, there are a few main approaches—two of which are outlined here.

The first, and perhaps more traditional, method is to establish a centralized database to replace various siloed databases, validated, cleansed and de-duplicated. This approach has a couple of drawbacks. One is that depending on the number of databases there are to replace—and that could easily number in the high hundreds, or thousands for enterprises—deployment could take years. Another drawback is that all the silos need to be rolled into the central repository in one go; adding more later isn't straightforward, "because of the structures and constraints in place," Butlin explains. Third, increasingly data is virtualized in many locations, complicating capture because the data only "rests" in a single place temporarily and for specific analysis purposes. Finally, there are other data regulations that would prohibit such a "master data set," including data sovereignty and data localization laws in Russia, China and other countries.

A second option is to build a metadata model of the data, wherever it sits, and go from there. The model acts as a "set of pointers," says Butlin, allowing data to stay where it's already stored and be called by API queries when needed. "It fits over the top of everything, so you can leave your existing business operations running in the way they are," he says. "You don't have to disrupt them."

Because this approach allows data to stay where it resides and uses APIs to query it, in an over-the-top federated data model, it's very much a non-disruptive approach. It is also flexible, allowing the model to start with a few data sources and gradually build out to include more. Deployment for this approach tends to be much faster: months rather than years.

BEYOND COMPLIANCE: THE BENEFITS OF GDPR

Earlier we discussed the penalties possible under GDPR and, until enforcement actions begin and there is evidence to the contrary, there is little to suggest regulators will treat violations with a light touch. Neither should the potential reputational fallout of violations be underestimated.

However, there are upsides to compliance besides escaping regulators' attention. In this section, we outline a few of those benefits beyond compliance itself.

- **CUSTOMER CONFIDENCE:** Consumers may voluntarily share a lot of their personal data with the organizations they patronize, but in doing so they have an expectation that their data will be protected. GDPR compliance is one external validator that this expectation is met. There's also an opportunity for companies to take ownership of the protections they place on personal data and communicate that clearly to customers to foster brand trust. Even some companies not necessarily subject to the regulation are considering using GDPR as a guidepost to enhance trust with their customers and their employees.

- **CUSTOMER ENGAGEMENT:** GDPR compliance alone will not necessarily bring businesses to a place where they can build a single view of the customer and enable omni-channel marketing or the kinds of digital customer engagement associated with it. The process of GDPR compliance described previously, however, is fundamentally similar to the steps involved in data quality improvement efforts that underpin digital customer engagement. Data quality lies at the heart of both. "GDPR takes you through a journey that gives you a really good understanding of the individual, your customer," says Butlin. "If you've got that good, solid individual quality data, then that can lead you to single-view product engagements.…It gives you the starting point."

- **INCIDENT RESPONSE:** Umerley, who leads incident response for Pitney Bowes, says one of the first challenges of any data breach event is quickly identifying what information has been exposed and how many people are involved. This challenge is complicated if there's little understanding of where data is stored. With GDPR compliance, "now you do have a view of your clients, your customers," he says. "Your ability to identify what's impacted in the event of a security incident becomes better."

- **RESPONSIVENESS TO OTHER DATA REGULATIONS:** In many ways, the GDPR is setting the tone for global privacy regulation. While the U.S. is unlikely to enact any similar regulations at the federal level in the current political climate, state legislatures are more likely to consider enacting GDPR-inspired regulations. Other large economies, including Australia and Asia-Pacific countries, are likely to fall in line with GDPR to protect their trading rights with the EU. In the U.S., the Privacy Shield goes some way to protecting cross-border data flows, but self-certified Privacy Shield compliance is not equivalent to GDPR compliance. In the near term, those that do comply with GDPR will be in a better position to respond to these kinds of future regulations that bring other territories into line.

- **INNOVATION OPPORTUNITIES:** Beyond enhancing customer engagement, investments in GDPR compliance, data quality and sophisticated analysis may allow businesses to understand their customers in more nuanced ways. In turn, they may discover new insights about customers that will reveal previously unrealized opportunities for innovation in products, services and use cases.

RSA INSURANCE GROUP: REACHING SUSTAINABLE COMPLIANCE

Gillian Tomlinson is the chief data officer for U.K.-based insurer RSA Insurance Group, which—in addition to its B2C and B2B insurance brands—provides the insurance backbone for other large U.K. suppliers. The company aims to reach a sustainable compliance position by May 2018. In her role, Tomlinson has been heavily involved in that effort. Forbes Insights spoke to her about some of the challenges and opportunities that GDPR presents. The following conversation has been edited for clarity and length.

WHAT HAVE BEEN SOME OF THE BIGGEST SHIFTS, IN TERMS OF DATA, THAT GDPR COMPLIANCE HAS REQUIRED RSA TO UNDERTAKE?

Two and a half years ago—and it is public knowledge—we suffered a breach. We worked very closely with the Information Commissioner's Office to really identify what we needed to do to ensure we could close the gaps and ensure robust protective measures were embedded. And we put a lot of investment [into] just running a program to be able to secure our estate on that basis.

While we were doing that, GDPR has been tabled in. Versus the Data Protection Act, [GDPR] is far more onerous on an organization to ensure we have additional controls, accountability, and also that we are basically [self]-reporting incidents. Now we're absolutely mandated that we report within 72 hours. So, a lot of the GDPR requirements [require us] to change our operating model internal systems, how they gather information, and what sort of security and protection measures we need.

IT SOUNDS LIKE GDPR IS A CONTINUATION OF A JOURNEY THAT RSA WAS ALREADY ON.

Yes, exactly. I think so for all companies, to be fair, because the Data Protection Act has been in place across the U.K. since 1998. So, protecting customers' information is not something new in terms of an organization having to implement the right controls, processes and accountability. However, there are [other] far stricter penalties, in terms of regulatory compliance. There is far greater focus across the board in terms of the reputational and financial impact [a breach] could have on an organization. And new technology and big data have changed the landscape and the way we need to manage data. So, I think what's actually happened is the legislation is catching up to changes in the market. For us as an organization, we've always seen [data protection] as a critical focus area to protect our customers and their rights.

IS THE SIZE OF THE POTENTIAL GDPR PENALTIES CONSIDERED A TOP RISK?

Not just the regulatory penalty, but the customer impact [in] both B2B and B2C. Under the B2B banner

> "There [are] definitely additional benefits that come with the security, the coordination, the control around these data that GDPR brings."
>
> **GILLIAN TOMLINSON,**
> CHIEF DATA OFFICER, RSA INSURANCE GROUP

we would lose the trust of the financial institutions who partner with us. Companies like ourselves invest heavily in marketing and our customer propositions. One breach could erode all that good investment. So, we're acutely aware of, let's say, the overall impact.

WHAT HAVE BEEN SOME OF THE BIGGEST CHALLENGES FOR RSA IN TERMS OF DATA COMPLIANCE?

There are a couple of things, really. One, we're a major insurance corporate organization that needs to ensure we retain data, not just specific to GDPR but to how we process claims and assess risk to provide the best proposition for our customers. We also have a fairly large estate in terms of systems, applications, processes and different ways for customers to engage our organization.

So, for example, one of the things from a major corporate [perspective]—and a lot of my colleagues in the market face this as well—is being able to look across an organization that runs in a certain way and look at the way technology has moved, and the way criminals are behaving in the market with new technology and tooling. [Then] being able to actually implement the right security measures, controls and processes, the right operational procedures across that estate because you are putting new processes into legacy areas. That's one of the key challenges that we face. It's all eminently doable, but it's a key challenge—requires a lot of investment, a lot of work—hence the fact that we've got a major transformation program underway specifically to ensure GDPR compliance.

There are probably two other things. One is ensuring that we fully understand what this compliance actually means, what is a sustainable position in terms of risk mitigation, because it's never a completely, 1,000% secure estate. It's an ongoing activity that needs to be fulfilled on an ongoing basis, whereby you're constantly challenging yourself, constantly checking to see if you've got a secure estate or you don't. And with that comes a new way of working. It's new information security teams, new ways of working in your operational teams; it's across your business. So, the education across your business, and really understanding and handling customer or personal data, is critical.

AND WHAT HAVE TURNED OUT TO BE SOME OF THE MOST VALUABLE ELEMENTS OF YOUR DATA STRATEGY FOR GDPR?

Having a formal program is absolutely key. I don't think you can do this through normal BAU [business as usual] mechanisms with any major corporate or company. Having sponsorship from the exec to get an amount of investments unlocked, to drive a formal program of work, has been probably the absolute starting point for us to be able to get proper traction.

DO YOU SEE A BENEFIT TO GDPR COMPLIANCE BEYOND THE FACT OF COMPLIANCE ITSELF?

Absolutely. A lot of organizations are still struggling to even get to a single customer view. This is one of those key legislative pieces that forces you to completely understand where your customer data is, how [to] bring it together, simplify your processes, ensure that you have robust controls in place and [introduce] more optimized mechanisms for how you manage data. [That] drives improved efficiencies around customer service and a lower operational cost base, therefore also allowing us as an organization to provide better customer propositions. There [are] definitely additional benefits that come with the security, the coordination, the control around these data that GDPR brings.

WHAT ADVICE DO YOU HAVE FOR OTHERS UNDERGOING OR EMBARKING UPON THEIR OWN GDPR COMPLIANCE EFFORTS?

It's not just a technology play. No technology solution is going to solve this legislative requirement. One of the biggest areas of focus needs to be around how you actually implement a dynamic operational model within the organization to sustain compliance and ensure the necessary safeguards are in place regardless of changes to the technology landscape or introduction of new innovations. And that covers training as to how

you respond to customers' requests, to how you report incidents and breaches, to accountabilities across the board. So, from my point of view, the advice would be that companies need to have a really, really strong focus on the operational change that's needed to ensure sustainable compliance—as opposed to the sorts of changes that come with implementing a specific technology solution or a set of controls that you're hoping the BAU environments will adopt as they are set up today.

IKNOW SOLUTIONS: THE VALUE OF QUALITY DATA

Amsterdam-based iKnow Solutions, a Pitney Bowes partner, offers enterprise-level data solutions to a customer base that spreads across Europe and the U.S., and spans industries from retail to financing. Forbes Insights spoke with Laura Eisenhardt, executive vice president, about GDPR and what businesses need to know. The following conversation has been edited for clarity and length.

WHAT ARE SOME OF YOUR CUSTOMERS' BIGGEST CONCERNS AROUND GDPR?

Customers are a little overwhelmed at the vastness of GDPR and all of the different aspects of it. A lot of them get bogged down with, "Where do I start?" And I get that, because it is complex.

HOW IS IT DIFFERENT FROM EXISTING DATA PROTECTION REGULATIONS IN PLACE?

GDPR goes way further than any previous regulations. You have to understand, there's been no new [EU] data regulation since 1995, and our world has changed a lot since then. Knowledge is vastly different, the way we communicate, and the amount of data that's collected—[it's] completely electronic. So, [GDPR] is vastly different from anything that has been in place before, and needed to be. The intent is just trying to give control back to the person whom the data is about, and if an individual entrusts you with their personal information, you need to guard it, and understand the value of it.

WHAT OBLIGATIONS WOULD YOU HIGHLIGHT UNDER GDPR FOR BUSINESSES?

Well, first and foremost, is that [you] need to know who [your] customer is. A few of the highlights of the GDPR ruling are that people have the right to know what information you have about them. They have the right to modify whatever information you have on them, they have the right to have you remove them from your system, and they have the right to be notified in case of a data breach. It's impossible

> "It's impossible to comply if you don't have a single vision of your customer."
>
> **LAURA EISENHARDT,**
> EXECUTIVE VICE PRESIDENT, IKNOW SOLUTIONS

to comply if you don't have a single vision of your customer or employee.

Let me give you an example. If I'm your customer, and I've been your customer any length of time, there's a good possibility that there's another Laura Eisenhardt pretty close to where I've lived. How do you know which Laura Eisenhardt I am? And if I ask you to tell me what you know about me, and you send me the data of a different Laura Eisenhardt, you just violated the GDPR. Or if I say, "remove me," how can you remove me if you don't know which one I am?

So, as a company, I want to have a single record of you to say who you are, where you live, maybe who is in your family. I want to know what things you've given me permission to keep, what things you've given me permission to contact you about. I need to have all that information about you in a single place. That is true whether I have a hundred million customers or I have 10. Obviously, there are a lot of other pieces that come into play, but that was really at the core for me of how we would go about implementing a GDPR solution, coupled with a robust data governance.

IS THERE VALUE TO GDPR COMPLIANCE BEYOND COMPLIANCE ITSELF?

Of course, there is the actual monetary value, aligned to the multiple fines. But now data quality matters for compliance, and with a high level of data quality comes the benefits attached to knowing your customer and being able to give exceptional customer service. Knowing your customers allows you to sell them products and services that fit their lives. Another benefit is the increase in consumer confidence. With so much of our business being done digitally, GDPR gives the opportunity to step into it, own it, and say, "We value you, and here's what we do [with your data]. We protect your data because the most important thing in our business is you." If a company can convey that level of integrity to its customers, consumer confidence will skyrocket. These are the actions that are going to make the difference between being an early adopter, complying, and being the company caught with blatant violations that then spends the next decade trying to recover their reputation.

DUN & BRADSTREET: DATA BEST PRACTICES

Anthony Scriffignano, Ph.D., is senior vice president and chief data scientist at Dun & Bradstreet. He regularly presents at global venues regarding emerging trends in data and information stewardship. Forbes Insights spoke with him for his perspective on data issues as GDPR approaches. The following conversation has been edited for clarity and length.

IS DATA QUALITY CONDUCIVE TO GDPR COMPLIANCE?

If you're focused on data quality, then you're focused on how you discover, curate and synthesize information. We talk about standards, accuracy, completeness—all of those things help you identify when you have personal identifying information, where you're keeping it, how you're storing it, and to some extent if you're protecting it. So, I don't think it's a 100% overlap, but I don't see data quality efforts working [counter] to efforts to comply with GDPR—I see them as very much complementary activities.

WHAT OBLIGATIONS UNDER GDPR STAND OUT AS IMPORTANT TO YOU?

It's important to understand what the definition of personal data is, what types of data are intended to be protected and the scope of that protection. Also, it is important to understand your role in the context of the data to be protected and the different responsibilities that come with your role. Are you a controller, a processor or a data protection officer? Finally, you must understand your own environment and be realistic about it. What do you have already? Can you honestly say that you understand the data that's in your data supply chain? Where it is and why it's there? And the reality is, for some organizations, they were struggling to answer those questions before GDPR was on the landscape.

WHAT KINDS OF DATA BEST PRACTICES CAN ORGANIZATIONS ADOPT TO BE MORE RESPONSIVE TO GDPR AND OTHER DATA PROTECTION REGULATIONS THAT MAY FOLLOW?

One thing I would say is all your processes should be a closed loop. There should never be a "one and done." There should be ongoing review. There should be ongoing reevaluation to make sure that when the environment changes, the response to that environment is changing in a commensurate way.

The second thing is to be very careful if you have the wolves watching the henhouse. There needs to be separation between the organization that's responsible for compliance and the one that's responsible for [data] discovery, curation and stewardship. You don't want to be entirely self-evaluating. That doesn't necessarily mean that you have to bring in auditors, but it means you should think about organizational allegiances and unintentional work at cross purposes.

The third thing is you should occasionally get an outside opinion in some way. That might mean you bring in consultants, it might mean that people attend training and seminars, or that you have customer forums. But you've got to have that external voice.

CONCLUSION AND TAKEAWAYS

GDPR represents the next step of an evolution in the way we, as a society, treat personal data and the obligations of organizations to protect it. The potential fines are designed to be dissuasive, but they're not the only reason to undertake compliance. Since it requires a level of good quality data practice, GDPR presents an opportunity to realize benefits beyond simple compliance: customer confidence, incident response, reputation and a foundation for new innovative products and services could be by-products of a well-thought-out GDPR implementation.

On the other hand, because so much is at risk—the penalties and reputational fallout have potentially devastating impacts—taking a "wait and see" approach is tempting fate on a grand scale.

Key takeaways:

- **BRING A MULTIDISCIPLINARY PERSPECTIVE:** GDPR compliance requires cross-disciplinary input, and all stakeholders should be called upon, from legal to IT to marketing. Give serious thought to who needs to be at the table.

- **UNDERSTAND DATA DISCOVERY AND CURATION REQUIREMENTS:** Before making any technology investments, organizations should understand what data they have, where it's stored and why, and what needs to be provided to the end customer. Know what can be done without. "You have to get a handle on that and apply the regulation appropriately," says Pitney Bowes' Umerley. "Understand, based on the context of your business and which regulations apply, what controls need to be put in place."

- **GOOD DATA BRINGS BENEFITS BEYOND COMPLIANCE:** GDPR compliance won't solve all problems, but it will put businesses in a good position to take advantage of further data quality initiatives. From there, it is possible to build toward deeper customer engagement, enabled with a single view of the customer. It also has benefits for incident responses, building customer trust and, as above, potential innovation opportunities.

- **IT'S NOT ABOUT THE BUSINESS, IT'S ABOUT THE CUSTOMER:** "Change your ideology so you understand that," says iKnow's Eisenhardt. "Understand that this is about valuing your customer." The GDPR enshrines the idea that personal data represents real people and has the ability to impact lives in tangible ways if misused. Compliance is less about checking off boxes than it is about taking to heart the responsibility of safeguarding peoples' data and using it transparently—and it should be approached accordingly.

- **START SMALL IF NECESSARY, BUT DO START:** "Don't underestimate the scope of this and how it might impact your organization," says Umerley. So, don't wait for the regulators to knock. If the task seems overwhelming, start small. "Go division by division, location by location," suggests Pitney Bowes' Berry. "Get the process moving and share results, rather than putting a five-year IT project in place. Take small steps, show progress, show consumers that you're taking action, and slowly roll those out across your business." These plans and progress can be proffered if regulators do come calling and want to see evidence of action.

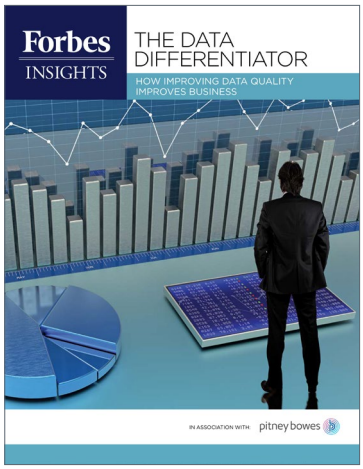
For more information about Pitney Bowes, the Craftsmen of Commerce, visit: **http://www.pitneybowes.com/us/gdpr-compliance.html**

ACKNOWLEDGMENTS

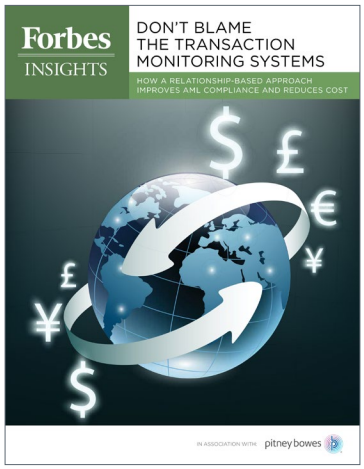
Forbes Insights and Pitney Bowes would like to thank the following individuals for their time and expertise:

- **Andy Berry,** Vice President, Europe, Middle East & Africa, Pitney Bowes Software
- **Chris Butlin,** Director, Professional Services Customer Information Management, Pitney Bowes
- **Laura Eisenhardt,** Executive Vice President, iKnow Solutions, North America, UK and EMEA
- **Ilya Meyzin,** Vice President and Data Science Chief of Staff, Dun & Bradstreet
- **Anthony Scriffignano,** Ph.D., Senior Vice President, Chief Data Scientist, Dun & Bradstreet
- **Gillian Tomlinson,** Chief Data Officer, RSA Insurance Group
- **Ray Umerley,** Vice President, Chief Data Protection Officer, Pitney Bowes

ADDITIONAL REPORTS FROM FORBES INSIGHTS AND PITNEY BOWES:



THE DATA DIFFERENTIATOR:
How Improving Data Quality Improves Business



DON'T BLAME THE TRANSACTION MONITORING SYSTEMS:
How a Relationship-Based Approach Improves AML Compliance and Reduces Cost

Forbes insights

ABOUT FORBES INSIGHTS

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 94 million business decision makers worldwide on a monthly basis. By leveraging proprietary databases of senior-level executives in the *Forbes* community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across *Forbes*' social and media platforms.

FORBES INSIGHTS

Bruce Rogers
CHIEF INSIGHTS OFFICER

Casey Zonfrilli
DIRECTOR, ACCOUNT MANAGEMENT

Tori Kreher
PROJECT MANAGER

Todd Della Rocca
PROJECT MANAGER

EDITORIAL

Erika Maguire
EXECUTIVE DIRECTOR

Kasia Wandycz Moreno DIRECTOR

Hugo S. Moreno DIRECTOR

Lynda Brendish REPORT AUTHOR

Zehava Pasternak DESIGNER

RESEARCH

Ross Gagnon DIRECTOR

Scott McGrath RESEARCH ANALYST

SALES

North America
Brian McLeod EXECUTIVE DIRECTOR
bmcleod@forbes.com

Matthew Muszala DIRECTOR
mmuszala@forbes.com

William Thompson MANAGER
wthompson@forbes.com

Kimberly Kurata SALES EXECUTIVE
kkurata@forbes.com

EMEA
Tibor Fuchsel MANAGER
tfuchsel@forbes.com

APAC
Serene Lee EXECUTIVE DIRECTOR
slee@forbesasia.com.sg