May 25 has come and gone, and **GDPR** is here to stay.

Now, companies face myriad issues tied to
data management, data security and data deletion — upon request, of course.
Welcome to the brave, new world of globally managed data.
In these virtual pages, payments industry heavyweights lay out what awaits.

TABLE OF CONTENTS

NEW REGULATORY CLIMATE

KARL KILB
Chief Executive Officer

Consumers around the world are now focusing more attention on who is collecting their personal data, why it is being collected and how it is being used and stored. The realization that personal data often gets into the wrong hands and leads to widespread fraud is creating a new regulatory climate. The General Data Protection Regulation (GDPR), adopted in Europe, is at the forefront of addressing such critical issues, and will force positive changes by holding companies accountable for how they collect, use and store personal data.

The internet has become the place for fraudsters to get and misuse personal data. Authentication that separates the consumer's identity verification and transaction validation from the internet is essential. A multifactor and multichannel approach to authentication that does not involve personal data is the best way to ensure [the information] is not compromised.

GDPR is designed to put an end to the unrestricted collection of customer data. For years, companies have aggregated customer data, and have operated under the belief that the aggregation of such data is allowed and inherently valuable. GDPR requires companies to justify their collection of customer data by having a legitimate interest in the data collected and providing adequate measures to secure the data. GDPR recognizes that the collection of customer data by companies places the customer at risk, because this information can later be compromised in a data breach. Once the data is compromised, the customer can be subject to identity theft and fraud. In light of the rising instances and costs of cyberattacks, GDPR mandates companies to reduce the amount of information they collect and to provide adequate protection for any sensitive information they retain.

[It also] clearly establishes that the aggregation of customer data can create tremendous liability. Companies that are not GDPR-compliant can be subject to penalties, as well as the damages and reputational harm that can flow from a data breach. For example, if a biometric database is compromised, the data can never be relied on again, creating catastrophic conditions for consumers and potentially large liability for the companies involved in the breach.

Ironically, [though] cybersecurity experts and regulators recognize the internet is inherently flawed, many authentication solutions require the customers to provide their most sensitive personal data — including their biometric information — in a manner that touches the internet. Such solutions are counterintuitive. The internet was built to allow for the easy

sharing of content, and not as a means of securing transactions.

Because the internet is inherently vulnerable, any authentication solution that relies on the internet is [also] insecure. The internet is a very dangerous place, especially when an application or site is a single point of failure. Any security that relies on the internet is inherently flawed, and any security that relies on encryption is subject to hacking. The internet is littered with personal data that was supposedly protected by encryption.

The "2017 State of Authentication Report," independently produced by Javelin Research and sponsored by the FIDO Alliance, correctly pointed out the many vulnerabilities of internet-based solutions and recommended that authentication involve multiple channels, in addition to multiple factors. Authentication must be separated from the transaction itself to provide real security. Regulations, such as GDPR in Europe, recognize that personal data must be protected with the greatest possible security. The best solution is to provide bullet-proof authentication without ever requiring, aggregating or storing personal data.

To demonstrate compliance with GDPR, and similar requirements that will be implemented in other regions, companies will need to prove they have received consents from customers concerning the collection, use and storage of their personal data. Authentication with an audit trail will also be essential to demonstrate this approval.

Boloro applauds the requirements of the GDPR, and is actively licensing our authentication technology to ensure compliance with it. Together, we can make the world a safer place by ensuring identity verification and eliminating fraud through a user-friendly, instantaneous, multichannel and multifactor approach.

GDPR'S BIG **SILVER LINING**

chargehound

ADRIAN SANDERS
Chief Executive Officer and Co-Founder

After years of discussion, negotiation and preparation, GDPR is finally upon us! As May comes to a close, businesses in every industry are bracing themselves for the impact of GDPR on their operations and growth. While GDPR might sound scary, the truth is that it's probably a good thing for all of us — both as humans and as companies — in the long run.

GDPR has broad implications, and parts of it can seem vague. This has created some uncertainty and unease, particularly among merchants who depend on highly personal customer data. [It] turns out that most consumer-facing merchants depend on this data — from eCommerce to ticketing, to booking and two-sided marketplaces.

So, what happens when these changes kick in? The effects of GDPR are impossible to predict entirely — but I can share the key ways in which Chargehound expects the new regulation to affect players in our space. Merchants with a strong technology culture will likely not face any major issues with GDPR, simply because it's easier to update modern infrastructure to handle the data privacy requirements. The bigger challenge will be for merchants that don't yet see technology as a core part of who they are what they do.

In the short term, GDPR necessitates operational changes.

There are real, punitive consequences for violating GDPR. That means merchants are taking it much more seriously than previous attempts to regulate, such as the European Data Privacy Directive (DPD). Right away, complying with GDPR requires more consultants, more audits, more security updates and more processes to be put in place. The single biggest issue for merchants in the short term is this: What is the best way to operationalize the processes necessary to become compliant? The bigger the merchant, the greater the need for more communication, training and monitoring. Smaller and newer merchants may see an advantage here, since the technologies they likely have in place are natively suited to meet GDPR requirements. Mature merchants will have some heavy lifting to do in order to get up to speed if their infrastructure is older and requires manual processes. Team leaders should see this as an opportunity to champion new overhauls in how their organizations process and handle data.

In the long term, merchants that embrace technology will secure a competitive advantage.

GDPR will force merchants to face the fact that they are now data companies in addition to their core offerings. Those companies that take

this challenge seriously will end up with a major competitive advantage in the years to come. The new requirements require merchants to turn toward technology and automation in order to stay compliant. Savvy leaders will see an opportunity to push for bleeding-edge updates to infrastructure, ultimately reducing expenses and bolstering margins. The rest will simply flounder, hesitant to grow market share rapidly for fear of incurring further penalties.

GDPR is an opportunity for merchants to modernize and embrace innovation.

It's always important to take challenges and use them as opportunities to reflect and dive deeper to understand where the future will take us. In the coming years, companies need to better understand how they manage data, who has access to it and what is expected of them. It's no easy task to understand the scale of what is required, [particularly] if you approach it from a non-technological perspective.

When we first started Chargehound in 2016, we were amazed at the amount of people handling chargeback representment manually. Now, after talking with hundreds of merchants, I understand the history and context of how manual solutions were put into place. In some cases, merchants are employing dozens of people to process thousands of disputes. In other cases, they've outsourced thousands of disputes to hundreds of subcontractors. Imagine the GDPR implications of having all those non-employees handling customer data! For some of our merchant partners, they might have had over 100 people handling and accessing personally identifiable information (PII) for thousands of customers each month.

By embracing automation technology, merchants have drastically reduced their GDPR scope and made it 100 times easier (literally) to manage. This is just one example of how GDPR can encourage merchants to capitalize on truly automated technology to solve issues of efficiency and scale.

GDPR requires merchants to become more responsible and organized when it comes to customer data.

There are only two ways to accomplish that goal. One way is for merchants to reduce their data footprint by slowing growth or pruning their customer base to a manageable size. The other, better, way is for merchants to update their technology infrastructure to securely process data and scale with growth. To do the latter requires a paradigm shift: a culture change that welcomes technology as an answer to challenges of scale.

Embracing that type of culture can be daunting and difficult at times, but in an era when 50,000 items can be sold in five minutes, those businesses [that] take the leap will continue to thrive. Merchants can prioritize such a culture shift now or later. If they wait too long, the GDPR penalties will be only half the problem — soon, they'll be left behind by the competition.

WHAT'S GOOD FOR YOUR **CUSTOMERS** IS GOOD FOR YOU

Entersekt

NEIL BESTER
Senior Vice President of Products

In an era where data — and not just actual money — holds real power, banks are finding themselves in an interesting position. Add to the equation new regulations requiring more care with asking for, using and storing consumers' data, and the situation can seem overwhelming. But, when approached resourcefully, complying with GDPR can actually help banks break new ground in terms of customer relationships and digital enablement.

The key requirements

Especially in the U.S., the issue of personal data remains an area of concern in the wake of numerous high-profile data breaches over the last few years. Consumers are slowly, but surely, becoming warier of sharing their data online as cybercrime and digital identity fraud continue to increase. Governing bodies, too, are playing it safe, and regulations like the European Union's GDPR are actually demanding that consumers have more say in who gains access to their data.

To comply with the requirements of GDPR, organizations that handle customer data need to make sure they implement the following measures, among others:

- Before using a customer's personal data, the organization must request that customers consent in an intelligible and easily accessible way. The customer must also be able to withdraw this consent easily.
- Customers, if they ask, must be informed if their personal data is being processed by the organization, and for what purpose.
- The organization may not refuse customers when they request a file of their personal data in order to give this data to a different organization.
- The organization must keep the data they store and process, as well as the number of persons [who] access this data, to an absolute minimum.
- Customers must be informed of a data breach within 72 hours of the organization becoming aware of the breach.
- The organization must, if the customer requests it or withdraws consent, erase [the] customer's personal data from its records and stop using or distributing his data.

Organizations that do not have these measures in place by May 25, 2018, can expect to be fined heavily — up to $23.6 million or 4 percent

of their total annual global turnover, whichever is highest. [Though] GDPR is a creation of the European Union, its requirements apply not only to organizations in Europe, but to any company that stores or processes the personal information of EU citizens.

The introduction of GDPR will mean better data protection — an undoubted win for consumers. For organizations, managing data kept on consumers — monitoring their consent to store and use their data, keeping track of where it is stored and who has access to it — will certainly prove challenging. With open banking also looming on the horizon, it could potentially get even more difficult in future. At first glance, GDPR may appear to bring nothing but trouble for organizations, [but] there is actually a long-term upside to it for them as well.

When an organization's brand is what customers see when they are asked for consent to use their personal data, the brand will be what they associate with the feeling of empowerment those requests give them. The branding will be a visual reminder of the fact that they are protected — they are in control. This creates a relationship of trust or, in the case of banks with existing relationships with customers, it allows the bank to strengthen that relationship.

A challenge and an opportunity

Central to a successful implementation of GDPR compliance will be how banks choose to ask customers for consent. We know that consumers have always been friction-averse, demanding convenience above all else. Even though recent statistics indicate this is changing, as data breaches and the growth in cybercrime make consumers more aware of cybersecurity, ease of use remains a top priority.

So, how would a bank prove it has its customers' consent without implementing a cumbersome contract, or a process that requires customers to work their way through a lengthy terms-and-conditions process? The good news is that being compliant with GDPR and asking for consent does not have to mean inconveniencing customers.

Through a solution that harnesses the potential of the mobile phone, the bank can request a customer's consent to use or access their data in a way that is convenient, secure and GDPR-compliant. Deploying digital certificate technology to the phone creates an out-of-band communication channel between [it and] the bank, over which requests can be sent securely. What's more, the customer's response is digitally signed, providing the bank non-repudiable proof of consent as required by GDPR. Customers can provide or refuse consent with the touch of a button on their phone, and they never have to be subjected to cumbersome and time-consuming authentication processes.

Once compliant, focusing on how to make the most of their customers' data can be a differentiating factor for banks — one that sets them apart from competitors and newcomers. The future-savvy bank will be able to leverage the data they have on their customers, and the enhanced level of trust generated by explicit consent, to become a trusted advisor and, in so doing, become the go-to place for all the customer's financial needs. Complying with GDPR can either be no more than bank's next regulatory headache, or it can offer them a whole new way of interacting with their customers — with an eye on the digital and data-driven future.

WELCOME TO GDPR – NOW WHAT?

FEATURE SPACE

DAVE EXCELL
Founder and Chief Technology Officer

Consumers' personal data rights have been a prominent discussion in recent years, and the activation of GDPR last week demonstrates how seriously the issue is being taken. The rules apply to organizations that collect data from EU residents, or that process the data of EU residents on behalf of a data controller, regardless of where the organization is located. Determined to protect the privacy of individual consumers in the digital age, European regulators are prepared to hold organizations that improperly manage and process personal data accountable, with a maximum penalty of 20 million euros (nearly $24 million USD) or 4 percent of the annual global turnover — whichever is higher.

There's no [way] that any company offering products or services to EU-based consumers can take GDPR compliance lightly, so why are so many U.S.-based organizations seemingly unprepared?

In a customer survey, Sage found that 91 percent of U.S. respondents currently lack awareness of GDPR, while 84 percent admitted to not understanding what it means for their businesses. In the U.K., the responses show 57 percent and 60 percent, respectively. Moreover, IBM reported that only 36 percent of surveyed executives say they will be fully compliant with GDPR by the enforcement date.

The immediate challenge

In the near term, GDPR can seem overwhelming because there are countless processes that place information within the scope of the new rules. It can be intimidating to even the most seasoned CISOs and information security leaders, because customer engagement, staff data information management and analytics strategies must all be evaluated to ensure overall compliance.

Organizations must identify all managed personal identifiable information (PII), which is a heavy task that involves mining and evaluating all available data archives. In addition, GDPR expanded the definition of what qualifies as personal data. In addition to names, emails, contact numbers and birthdates, things like IP addresses, cookie data and mobile device IDs will be included. Basically, any information that can be used to identify an individual — either on its own or when combined with another piece of information — must be vetted, and the organization must prove that it satisfies one of the following standards for processing:

- *Consent:*
  The consumer has been provided a choice to opt-in or opt-out of the use of his or her data.

- *Contract:*
  The data is to fulfill a contractual obligation, or the consumer has provided the data in preparation to enter a contract.

- *Legal obligation:*
  The data is in accordance with a specific legal obligation to which the organization is subject.

- *Legitimate interests:*
  The data is necessary to achieve a legitimate interest, when balanced against the consumer's interests, rights and freedoms.

- *Public task:*
  The data is necessary to perform a task carried out in the public interest.

- *Vital interests:*
  The data is necessary to protect or preserve the life of a person.

Approaches will vary. For example, not every organization is required to hire a data processing officer (DPO). According to the Information Commissioner's Office, the U.K.'s regulatory body that upholds information rights in the public interest, companies carrying out large scale systematic monitoring of individuals (i.e. online behavior tracking) or large-scale processing of special categories of data, or data relating to criminal convictions or offenses, are [all] required to appoint a DPO.

Discovering the data and determining its accuracy remains one of the most critically challenging components of GDPR.

Learning as we go

As with all new rules, there will be some gray areas with GDPR. Take enforcement, for instance. Because it is a new set of rules, the industry lacks historical perspective on how each violation will be interpreted by the courts.

In the U.K., a consumer's request to have his or her PII erased must be obliged by the controller "without undue delay," but the U.S. has laws that directly conflict with this. The Bank Secrecy Act requires that "customer identifying information obtained in the account opening process" be retained for five years. This could put data collectors, processors and financial institutions in a difficult position.

Consider the issue of third parties and partners. How can companies be sure that *they* are taking it seriously and will remain compliant? And, upon which entity does the responsibility fall? Financial institutions will need to know how to exercise a new dimension of due diligence to properly determine if a supplier can effectively enable GDPR compliance, and [do so] without causing any disruption to the day-to-day processes and operations.

From a budgeting standpoint, what will the impact of increased documentation mean for organizations' balance sheets? Operationally, the requirements will likely incur new costs and introduce time-intensive practices that stem from training, policy development and other essential oversights.

What's next: post-GDPR

We'll have to be patient before the long-term impacts of GDPR become ostensible, but some near-term changes stemming from the new rules could include:

- *Improved third-party management of practices:*
  Internally speaking, intensified data oversight requirements could potentially lead to the re-evaluation of third-party management practices, which could result in the consolidation of technologies to mitigate risk and increase control. When prospecting organizations for potential partnerships, the evaluation of GDPR synergies will be an important step to confirming the necessary levels of transparency, [especially] in terms of how data is being used and managed.

- *Greater consumer-facing awareness for compliance:*
  The changes could redefine the role of compliance in the public eye. Now, GDPR abidance will be a strong proof point for consumers in selecting who they do

business with and who they trust with their data. Establishing a strong reputation as a GDPR-compliant organization also serves to drive new business, as the value and importance of aligning with trustworthy partners will increase. This creates an opportunity to reinforce a key differentiator or expand into new markets altogether. Conversely, an organization's inability to comply, even once, could drive customers and partners away — and do irreparable damage to its reputation within the industry.

- *Closer relationships between marketing and IT:*
  With GDPR, the nature of the customer relationship is centered around privacy, which is a departure from today's conventional marketing wisdom. Long ago, getting in front of potential buyers was organic, as both parties were interested in learning more about each other. With the digital age, the relationship has become unbalanced, and consumers are bombarded with information that they don't necessarily want or need. Now, marketing efforts will need to align with IT capabilities to both build relationships and remain compliant.

Finally, one of the biggest impacts could potentially be on cultural governance. An organization that isn't already acting in the best interest of its customers is more likely to reconsider its approach within the GDPR framework and all of its potential changes — perhaps resulting in one of the most significant changes to our industry.

DO NOT
COLLECT
WHAT YOU
DO NOT
NEED

ROBERT PACE
Vice President of Information Security and Compliance

Throughout its 11 chapters and 99 sub-articles, the overarching intent of this regulation is straightforward — to protect consumer data. As a payment processor, that responsibility impacts everyone working in payments.

[Though] it remains to be seen how regulators will enforce GDPR, and what they collectively view as a reasonable level of compliance, that is no reason to take a wait-and-see approach.

At First American Payment Systems, we are engaged in processes to align with these new regulations. The nature of payments, commerce and overall financial services requires us to evaluate and enhance the processes for conducting business. It is not that the good and/or service itself is changing, but rather how companies treat the related consumer data. This also means companies have greater responsibility in protecting consumer data, regardless of where they are headquartered.

As GDPR becomes more established, there are several articles that could spark innovation in the marketplace. Two examples are Articles 25 and 32.

The first focuses on data protection by design and default, and carries with it an enhancement to the controls on the data collected. We must ensure that, for the entire life cycle [of] any customer data that resides in the company's system, all employees with access to the data are referencing only the information they need for business processing (data minimization).

Article 32 covers security of processing — more specifically, how companies must protect the privacy of an individual consumer via security measures. It references "state of the art." This phrase bears mention because, in the context of regulatory language, security phrasing is typically more focused on baseline requirements. Here, the performance standard is much higher.

My fellow security practitioners will appreciate the fact that these regulations are supporting security as a first priority, rather than an afterthought. I think we can all expect regulators to hold us to the highest possible security standards, and that those expectations will evolve over time. That means our work as protectors of consumer data is never done. As innovation drives more effective business and security processes, companies are going to have to keep up. It's a shared responsibility and not just limited to technology.

As for the grey areas, these regulations will mature over time. The companies that set themselves up for GDPR success will

understand and be patient with [the] process, all the while demonstrating work to meet regulatory expectations as they are known today. Waiting for full guidance is not an option. Indeed, the companies that postpone efforts to implement GDPR directives are at [the] greatest risk. They may face severe financial penalties, as outlined in the regulation detail.

Avoiding that scenario starts now, with companies infusing focus into their respective security, privacy and compliance programs, and being transparent about the processes they are using.

RULES OF COMPLIANCE

GEOBRIDGE

JASON WAY
Chief Technology Officer

One thing in common among all possible compliance mandates is that adherence requires substantial investment and commitment for any enterprise. GDPR will be no different than any of its other related predecessors. Compliance is a "yes" or "no" proposition. An entity is either compliant or it is not. Interpretation introduces the appearance of [a] "grey" area.

However, "interpretation" is often offered by a well-educated subject matter expert [who] can build a case to justify a pro or con. Just like any high-profile crime drama, where the prosecution and the defense can introduce so-called "expert witnesses" who will portray an interpretation that favors the client, compliance interpretation, for any given industry mandate, is no different.

GDPR is about data security. One of the most prestigious certifications an IT professional can obtain is the certification as a Certified Information Systems Security Professional (CISSP(R)). One of the original domains of expertise to achieve a CISSP(R) certification was the discipline of Risk Management. To pass the exam [and] achieve this certification, an IT security professional must become aware of the mathematical formula that portrays a cost/benefit analysis with the acceptance of risk.

To illustrate a simple example, suppose a requirement existed that said every network hop necessitated the presence of an intrusion prevention system. Upon evaluation, the business determined that satisfying this requirement would necessitate a $500,000 expenditure due to the size of its infrastructure. However, failure to comply with the mandate yields a $25,000 fine. Now, this is a ridiculously simple example to prove the point, but the point is that no enterprise can justify spending $500,000 to avoid a $25,000 fine.

Risk management principles, notwithstanding mature and responsible enterprises, will endeavor to meet the minimum spirit of compliance with GDPR requirements. When "grey" areas arise, "expert witnesses" will be drawn upon in the spirit of begging [for] forgiveness in lieu of requesting permission, because no entity has yet to be fined as a result of a GDPR violation. The well-educated risk management professionals will guide their enterprise on the side of caution as it relates to compliance expenditure. Many enterprises have demonstrated a desire to be leaders that set examples for how to prepare, as opposed to followers [that] will struggle to catch up.

One of the few concepts that is easier to understand — among the hundreds of

thousands of words that make up the GDPR mandate — is "the right to be forgotten." Few are required to dig in deeper with the intent to understand what this means. It means that if I stop doing business with someone, and I don't want them to have my information any longer, they must guarantee that they forgot I ever existed. My historical transactions with this entity should not surface, years later, to ruin my financial well-being. This mandate, among all others, is the easiest to understand and is almost prescriptive for what would be required in order to achieve compliance.

An enterprise should do everything in its power to eliminate the re-production of personally identifiable information, including account information. Tokenization is the natural answer to this mandate. The concept of tokenization means that, rather than copy an individual's Social Security number in 23 different locations for various use cases, a single token value will be distributed to those 23 locations and the true clear data will be properly protected in a single location.

The most fantastic benefit of this requirement is that it applies in an absolute fashion. An enterprise must have, and be able to demonstrate, complete confidence that a single token value is truly representative of all possible storage locations — without errantly deleting a shared value that would otherwise prevent services for a duplicate owner of the same token value. For too long, tokenization has been deployed without standard. Tokens should be truly random or unpredictable, and they must be unique. Hundreds of software-based, pseudo-random tokenization solutions exist within the marketplace. The importance and absolute assurance to produce unique and unpredictable token values will drive enterprises to adopt more secure solutions, ultimately separating the wheat from the proverbial chafe. IT professionals will be forced to make more educated decisions and leverage legitimate solutions above and beyond deploying buzz word offerings. This phenomenon will prove to be positive for the industry as a whole, as it causes all solution manufacturers to dig deeper, try harder and offer more complete solutions in a non-standardized solution space like tokenization.

PRIVACY IS THE NEW NORMAL

MARK THOMPSON
Global Privacy Lead

Personal information is at the heart of the digital economy. Financial institutions increasingly rely on customers' personal information in the delivery of products and services, while customers value the customization, discounts and other benefits that sharing this data can allow. However, with new regulations like the European Union's GDPR coming into play, financial institutions must respond to meet regulators' requirements and maintain customers' trust.

[Though] the GDPR represents the largest changes to rules governing data protection in 20 years, these regulations are not an overhaul of current privacy and data protection laws. Instead, they add granularity and specificity to the rule set. Key changes to current processes as a result of GDPR include:

- Increased individual data rights. Individuals have the right to request copies of their data for free, delete data and obtain their data in a machine-readable format.

- Extra-territorial scope. GDPR applies to all entities providing a product or service to an EU subject, regardless of company location.

- Increased regulator powers. European regulators will gain broader powers, including powers to audit, cease processing and impose fines.

- Increase in liability. Regulators can now pursue organizations that process information on the controller's behalf.

- Data protection officers. Organizations must have a data protection officer to represent the individual's interests, and who must report any violation, loss of personal information or other breach of data security to regulators.

As a result of these changes, processes surrounding the collection, use and storage of customers' private information cannot be an afterthought. Instead, privacy and data protection must be at the heart of organizations' strategies, and a core component of any digital transformation or initiative.

GDPR compliance as a competitive opportunity

GDPR and the penalties for violation or non-compliance have received significant press in recent months — and for good reason. In contrast to some current data privacy regulations, violations of which may result in

a fine of €500,000, a serious GDPR violation might result in a fine of 2 to 4 percent of global turnover. This potentially hefty price tag has understandably made organizations cautious.

Yet, along with financial risk comes the possibility of reward. In responding to GDPR — and communicating clearly to customers about what data you collect, how data is used and stored and your planned response to data loss — you can increase customer trust. As we have seen in recent years, the trend in financial services is toward a more personalized, customer-centric model of product and service delivery. For these products and services to be successful, financial institutions must not only engender customer trust, but maintain and reinforce that trust over time through the effective safeguarding of personal information and appropriate responses to data loss. As customer trust and total volumes of customer data increase correspondingly, organizations will find they are better able to understand and target specific customer demographics, enabling more responsive marketing efforts and reducing wasted spend.

Responding to GDPR — now and in the future

Advice for financial institutions coming to understand this new regulatory landscape includes:

1. *Ensuring company leadership understands data as an asset and liability.*
   In recent years, data is often talked about as a valuable resource, similar to oil — yet this comparison is off base. Data is potentially far more valuable, yet it comes with greater business and operational complexities, as well as associated liability risks. For financial institutions operating in this new age, it is imperative for the board and C-suite executives to have a clear understanding of the value of personal data and its uses within the organization.

2. *Building an approach based on identified risk.*
   Privacy risks will look different for different financial institutions based on sub-sector, market, client base, technologies, current products/services and other factors. For example, the data protection strategy for an institutional investor may be less complex than that of an insurer or asset manager, given their more limited access to personal data. Companies need to carefully assess where data privacy risks exist across their value chain, and evaluate the appropriate level of control needed to effectively manage those risks.

3. *Taking the long-term view.*
   Effectively managing privacy compliance risk, whether in response to GDPR or other privacy legislation, is not a "set it and forget it" task. Data has become a critical component of any business in a digital age. Correspondingly, effective management of the company's collection, use and storage of personal data, as well as the associated risks, must become the new standard. Financial institutions should look to create sustainable privacy management strategies that can grow with the organization as digital products and online service delivery platforms continue to expand.

[Though] GDPR compliance looks different for organizations across the financial services sector, there is one constant: Financial institutions must respond to the regulatory pressure of GDPR and its mandate to protect customers' personal data. As technology increasingly drives innovation and growth strategies, effective data management and protection will become an integral component of competitive differentiation and long-term success.

LIABILITIES, GREY AREAS AND EVERYTHING IN BETWEEN

P97

STEVE MOSES

Senior Vice President of Compliance

The short-term impact of GDPR will be the heightened awareness of the maintenance of updated privacy protocols, [particularly those] regarding the control of customer data. Also, an updated definition of what constitutes personally identifiable information [is] moving from a triangulation approach to find or impersonate someone and toward essentially any piece of data that can be used to contact a person — a much broader definition. Fundamentally, this means any exposing of customer data can create a liability for a company. Companies [that] choose to err on the side of caution will take care to even hide this data from departments, such as customer support, to avoid even well-meaning employees from accidentally exposing PII.

As a result, this will mean a requirement for greater patience on behalf of consumers when calling for customer support. PII is likely to be well-hidden and, therefore, new means of identifying and providing support for things like financial transactions will have to be developed. Longer term, as companies and consumers become more comfortable with this "new normal," all parties will find efficiencies in how best to hide certain identification of a customer/consumer. [They must use] probabilistic methods to insure the near-certainty of the owner of information, such as in transactions, without necessarily ever knowing the true identity of the person.

Payments, commerce and financial services firms will still be driven by card issuer's requirements for transaction management. Just as in the payments business, when the concept of tokenization was developed to protect personal account numbers (PANs), PII will likely move to a tokenization scheme to protect identities. The sharing and/or selling of PII is likely to become much stricter, with greater emphasis [on] using the GDPR concept of data [on behalf of the] controller to protect data, rather than data protection always being a matter of a well-protected processor database of information. Additionally, with greater emphasis being put on the granting and rescinding of consumer permission to use data, companies will be required to truly take an active role [in] data protection.

Data privacy is likely to take on a global perspective, since GDPR endeavors to protect identity, [especially] if the data subject is an EU resident [and] regardless of data location. This will encourage adoption of the EU standards for GDPR [in] countries outside of the EU as a matter of consistency. Respect for local law — embedded in GDPR — will certainly cause some conflicts between GDPR and local law, which has the potential to be exploited. On the other hand, rules for the transport of PII out of

the EU may influence these and other related decisions.

Companies that are thought leaders will move to individualizing knowledge of consumers without personalizing the knowledge. That is to say, a similar approach used in the payment industry with tokenization will likely be fit to manage identity. Companies will find that, apart from very targeted direct marketing, individual demographic knowledge of an individual customer or consumer will provide high-quality, essential marketing knowledge, while providing the opportunity for protecting identity at levels that satisfy GDPR.

The companies with the most to lose will be those [that] are cavalier in their handling and/or sale of personal data. These companies may suffer both the financial penalties for violating GDPR, which can be substantial, as well as the reputational losses that will be inevitable and will undoubtedly take significant amounts of time to win back. The winners will ultimately be the consumers, whose privacy will be better guarded by those entrusted with this data, as well as companies [that] make privacy protection part of their daily business and embed this functionality into daily work processes. This will provide both a technological and security edge for these companies.

The obvious grey areas will be the possibility of enforcing GDPR in countries outside of the EU based on the protection of EU citizens. These situations are likely to run into conflicts between local law and GDPR, where local law does not recognize GDPR definitions of PII as consistent with local definitions of PII.

SELF-ASSESSED MOMENT OF **TRUTH**

riskified

EIDO GAL
Chief Executive Officer

In the short term, we'll see a number of companies indicating that they already were GDPR-compliant or that they've recently made changes to be so, but that's one of the many ways GDPR is tricky. Because this is a self-assessment process, the changes these organizations have made are entirely self-reported. That means the impact on consumers in the short term is unknown. We've had two years from adoption to enforcement, so this certainly shouldn't sneak up on anyone, but we won't truly know the impact until investigations take place and organizations are cited and fined.

The long term is more difficult. It's possible that regulators will take organizations at their word in their self-reporting, and everyone will breathe a sigh of relief, or it's possible that regulators will go after everyone and many organizations will face serious fines and changes. What we think is most likely, however, is that regulators will go after those organizations wielding significant power or acting particularly irresponsibly. They'll face serious repercussions, and the lines will be more clearly drawn.

Perhaps the biggest question, though, is what this will do for consumers. Consumers will get used to seeing longer and more in-depth privacy policies, perhaps even checking many boxes for disclosure, consent and the like. The hope is that this improves privacy and security as everyone pays more attention, but it's just as possible that apathy will win out and little will change.

We expect all these firms to be cautious, with the largest players taking the largest steps to ensure compliance. This includes not only EU-based organizations, but just about any organization that serves EU member countries, and even some that *might* serve EU countries. The potential penalties for not following the GDPR are very substantial, and the pain [this] would cause is much more significant than the difficulty of compliance requirements as we see them. We expect that we'll see a lot more organizations disclosing how data is used and for what purpose.

We wouldn't be surprised to see a cottage industry spring up, devoted to GDPR compliance and best practices. This certainly could include management of the technical aspects necessary to comply, but it also might involve marketing or consulting firms that help businesses conduct outreach in customer-friendly ways. We're looking forward to the first business to put out a truly funny GDPR disclosure form, because you know that's coming.

The organizations that have the most to lose are those that probably *should* have the most to lose. One of the most important distinctions about GDPR is the language around "legitimate interests." Organizations that have a real reason to collect and process data, and provide [a] genuine service, should be fine. It's those other organizations that are likely to be in trouble. Those organizations will likely face challenges as they either fail to disclose what they're doing and why, or they now ask for consent that is unlikely to come.

As to who has the most to gain, [those are] the organizations that have been doing things the right way. GDPR enforcement should eliminate the advantages less scrupulous organizations have enjoyed. Organizations will now need a real, legitimate reason to gather and process data, or else they'll be required to disclose and request consent. For the organizations that don't have a good reason to do what they're doing, this will be a real problem. And, as they lose prominence, as a result, legitimate organizations should benefit.

As a company that works in that space, we would certainly welcome more clarity, but it has been slow in coming. We specifically see disclosure of vendor relationships as a grey area.

Many organizations use third-party service providers for a number of legitimate reasons. GDPR clearly calls for transparency at large, but detailed transparency could risk the merchant's assets and make it more difficult to implement quick, efficient changes. Beyond that, many are debating whether they need affirmative consent to legally conduct their processing or whether they can rely on a legitimate interest. The boundaries of these issues — [the] level of disclosure required, [which] is, in fact, a legitimate interest for processing information and requires the almighty consent — could be clearer. Regulation based on subjective language is a cause for concern [in] any business.

The final concern is that GDPR wasn't built for organizations that fight fraud, and we'll have to navigate that. For example, the "right to be forgotten," [the] "right to erasure," of GDPR is a great tool for consumers, but it also has the potential to be a great tool for fraudsters, who want nothing more than to be forgotten. That's a difficult balance to strike, and there is no "GDPR hotline."

Fraud certainly isn't going away, and we don't want this to create vulnerabilities that fraudsters can exploit. We remain committed to approving good orders and avoiding fraud. We're going to work to collect the absolute minimum amount of data possible to effectively provide our service. We'll be as responsible as possible with [the] data, and we'll disclose whatever is needed while working to continue to provide a good customer experience.

CONTINUOUS **GDPR** COMPLIANCE

TOKENEX

JOHN NOLTENSMEYER
Head of Privacy and Compliance Solutions

Now that the May 25, 2018, implementation date for the GDPR is behind us, it's important to note that this is only the beginning. Complying with the GDPR will be an ongoing project and, as EU data protection authorities (DPAs) begin enforcing the regulation, there are a number of essential activities for maintaining compliance.

First, implement pseudonymization to protect the personal data your organization holds. The GDPR is intentionally non-prescriptive when it comes to technical controls. Given the length of time it took to write, pass and implement the regulation, specific technical controls would likely have been outdated before the GDPR enforcement date. However, there are multiple references within the GDPR to data pseudonymization as an appropriate technical measure to protect personal data.

Pseudonymization, replacing sensitive data with pseudonyms, is synonymous with tokenization, [or] replacing sensitive data with tokens. Tokenization has been utilized by the payment card industry for years to protect credit card data. The same technology can be applied to the identifying elements of personal data. Unlike encrypted data, which remains resident within your environment, pseudonymization can be used to completely remove sensitive data from your systems via a cloud tokenization provider. In the event the original data is required for processing, it can be temporarily detokenized.

A second critical GDPR activity is the documentation of your compliance efforts. Article 5(1) of the GDPR details personal data protection principles — lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality. Article 5(2) then goes on to hold data controllers explicitly accountable: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')." Unfortunately, simply doing all the right things won't be enough under the GDPR. You must also be able to provide evidence that you are doing them. Documentation that you comply with an existing data security framework can be used to demonstrate to other organizations and data subjects, as well as DPAs, that you are considering data protection by design and by default.

A third activity you should strongly consider is signing up for a code of conduct or certification mechanism as a method of demonstrating your GDPR compliance efforts. Article 40 encourages EU member states and the European Commission, as well as "associations

and other bodies representing categories of controllers or processors," to draw up codes of conduct. There are multiple benefits to subscribing to a code of conduct, including the demonstration of your commitment to protecting personal data and abiding by the GDPR. This gives other organizations and individuals an expectation that you can be trusted with their information.

Codes of conduct provide a level of mitigation against punitive enforcement actions by a data protection authority. Article 83(2)(j) mentions adherence to approved codes of conduct or approved certification mechanisms as potential mitigating factors when considering administrative fines.

The establishment of data protection certification mechanisms is contained in Article 42, along with "data protection seals and marks, for the purpose of demonstrating compliance with the Regulation." Certification provides the same benefits of a code of conduct, but can also be used by an organization to demonstrate compliance with Article 25, "data protection by design and by default," as well as a basis for international data transfers.

There are multiple certifications and codes of conduct available today. Unfortunately, none of them are yet to be officially approved by a supervisory authority or the European Commission.

Remember that May 25 wasn't a finish line. Enforcement of the GDPR is just the beginning an effort to standardize data protection laws across Europe, [which] will have a ripple effect across countries worldwide. Continue your compliance efforts with existing data protection frameworks while watching for official approval of GDPR certifications and codes of conduct. If you're not already using tokenization to pseudonymize the personal data in your organization, it's not too late to start.

PREPARING YOUR CROSS-BORDER PAYMENTS PROGRAM

BRENT CRIDER
Director of Compliance

On May 25, the EU's General Data Protection Regulation (GDPR) will drastically change the cross-border payments landscape. The mandate has far-reaching compliance implications that affect how global financial institutions process data and move it across borders, including the data attached to capital transactions.

Cross-border payment providers that help companies manage international transactions must adjust their services in order to satisfy these jurisdictional changes around data security, both for themselves and as a watchdog for their clients. GDPR requires extensive reviews of providers' data protection management systems and their clients' territorial scope, not to mention the rollout of new privacy policies and the hiring of a data protection officer.

Vendors that manage payroll or payouts to contractors for their enterprise clients must be particularly vigilant about GDPR compliance, especially given the amount of personally identifiable information that accompanies these types of payments. Human resources and payments professionals who process employee salaries typically manage sensitive details, ranging from Social Security and bank account numbers to addresses, phone numbers and other unique tax information.

For compliance officers with cross-border payments accountability, here are the most pressing areas they must prioritize to ensure their enterprise has laid the best foundation for a new era of empowered consumers and privacy management:

Communication across departments

GDPR's 72-hour window for reporting breaches of enterprise data has drastically altered the timelines [to which] companies with European Union interests previously adhered. Legal, compliance, operations, information technology (IT) and information security teams must work collaboratively to ensure they meet all the regulatory obligations detailed in GDPR, without compromising on business performance. The best format for this alliance will lift certain elements from crisis response teams, law enforcement groups and even the military. The key elements worth extracting from these groups include a reporting group email, organized process documents that detail how information will be distributed and the assignment of specific roles and responsibilities to create a decision-making hierarchy best equipped to meet reporting requirements. Applying these features will strengthen a company's ability to observe, orient, decide and act swiftly to meet data protection obligations.

Recognizing the talent and technologies that enable positive change

To ensure GDPR compliance, cross-border payments firms must hire a data protection officer, one who ideally has experience orchestrating and assembling cross-enterprise committees in a timely fashion that minimize risk of exposure. Within these groups, the data protection officer must recognize and leverage the unique qualifications and knowledge sets available to help organizations interpret data protection laws, manage data from across the enterprise, identify the operational and infrastructure changes needed to mitigate liability and ensure this epic mandate does not compromise business performance or revenue streams.

Suffice it to say, the times of siloed compliance departments "bolting on" to an organization are over. Through people and technology, compliance must now become a strategic priority to uphold a company's financial well-being.

Applying proactive risk assessment

To ensure company liabilities are mitigated, regular preventative risk analysis and the internal review of information — in conjunction with IT and security teams — are a must in this new era of proactive compliance.

For example, the antiquated tick-box disclosure statements we see so often today must now reflect active acknowledgement by the customer. At the same time, contracts must be updated to reflect how information is stored and processed under a new regime, as well as confirm how firms sharing data are able to secure it while in transit. This rings particularly true in organizations committed to making cross-border payments with accompanying payer/payee datasets.

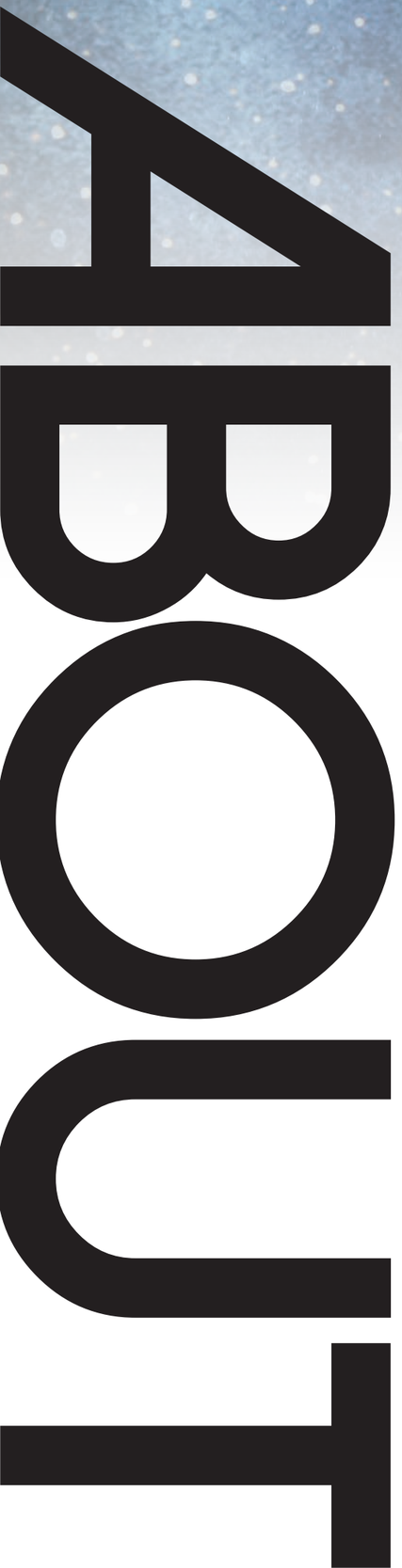
Understanding the 'right to be forgotten'

Under GDPR, customers now have the right to request "erasure" of their personal data from an organization's database. Whether it is a protected ID number or a simple email address, the organization is now required to fulfil the request and delete the data. For organizations leveraging archived data for business intelligence, such as how recipients prefer to receive payments from overseas, this is no easy process. Legacy archives, scattered backup stores and patchwork systems — following years of expansion, mergers and consolidation — fuel the daunting task of retroactively mapping data.

If there is any hesitation among colleagues about whether certain datasets should be removed, it is important to realize that most legal cases over this right end in the data subject's favor. Understanding the practicalities and exceptions for the "right to be forgotten" can help a compliance professional allocate their resources more effectively. For example, conducting historical or scientific research, or implementing employee work checks required for audit purposes, may not require deletion of data. For companies that exchange data with partners worldwide, especially, every ounce of compliance bandwidth that can be salvaged is valuable.

Conclusion

While the value of a growing globalized economy — catalyzed by rapid advances in enterprise and communications technology — cannot be denied, the prospect of managing cross-border payments data over a large volume of stakeholders is a daunting one. Amid instability and frantic preparation for GDPR, however, establishing a basis of improved communication, designated roles, robust technology and preventative action gives compliance professionals the best footing possible to meet and exceed these great expectations.



PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.