HOW TO TURN PROPER DATA MANAGEMENT INTO A COMPETITIVE ADVANTAGE

THE GLOBAL IMPACTS AND OPPORTUNITIES OF THE GDPR

JUNE 3, 2018

GDPREDGE YOUR ENTERPRISE COMPLIANCE SOLUTION

WHO IS THIS WHITEPAPER FOR?

1. For business stakeholders interested in understanding the GDPR and its implications for companies around the world
2. For the CISO, CIO, DPO or CEO trying to build a case for instituting proper privacy policy and systems at his or her company.
3. For data privacy stakeholder(s) looking for technology solutions to help operationalize GDPR compliance

"The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years."

www.eugdpr.org

CONTRIBUTORS

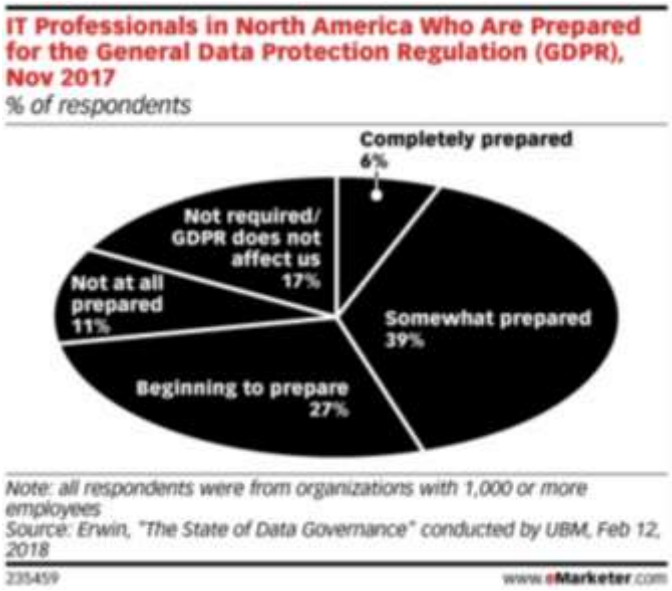
CONTENTS

OVERVIEW

Any organization that deals with the personal data of a European citizen (also referred to as a "data subject") has had May 25th, 2018 noted on its calendar for some time. This is the date when the comprehensive regulation and personal privacy framework came into effect. The General Data Protection Regulation (GDPR)—88 pages long and almost a decade in the making—not only defines privacy and how to evaluate whether an organization is properly protecting it, but also sets out consequences with substantial financial penalties for non-compliance.

With eMarketer reporting in March 2018 that only 6% of organizations are "completely prepared" for GDPR compliance, levels of anxiety are understandably high.

With data living in so many facets of any modern business—between the people that access it and solutions that analyze, store, and protect it—it is no wonder business leaders are, in many ways, overwhelmed trying to understand the task at hand.



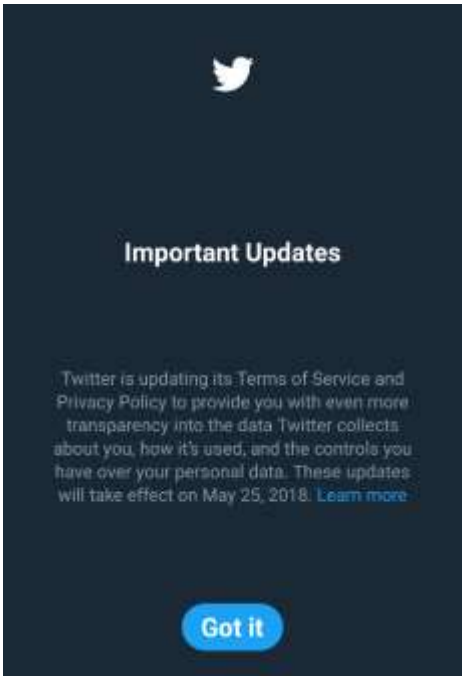
This paper sets out to give a high-level overview of the frameworks of the GDPR, the ramifications in and out of Europe, solutions to help achieve compliance and, most importantly, the opportunities that complying with the regulation will create.

> ***"Privacy is a human right – and we are obligated to enable our customers to fulfill that right."***
>
> *Satya Nadella, CEO Microsoft*

DOES THE GDPR APPLY TO MY COMPANY?

Before we explore the main tenets of the GDPR, let us first explore who needs to be concerned with these regulations. *Charles Morgan, Partner and Technology Practice Lead at McCarthy Tetrault* recently presented at a Canadian seminar on GDPR preparedness.

According to Morgan, "The GDPR applies not only to EU-established organizations that process personal data, but also to non-EU established organizations that target or monitor EU data subjects in one of two ways: either a) by offering goods and services to EU data subjects (payment not required); or b) by monitoring the behavior of EU data subjects (whether as customers, potential customers or employees)." This means that factors that are considered in order to determine whether an organization is "established" in the EU include whether the organization has a permanent local presence in an EU member state and whether it exercises a real and effective activity there, even a minimal one. For example, a company that has a sales representative, a mailbox and a bank account in an EU member state and that has a website offering goods in a local EU language would be subject to the GDPR.



For non-EU based establishments that process personal data of European "data subjects", Morgan laid out the other factors that could establish a need for your organization to comply:

- Whether the business offers goods or services in an EU language or currency
- Whether the business allows EU data subjects to place orders in the local language
- Whether the business refers to EU customers when marketing its goods and services
- Other evidence may show intent to target EU data subjects including, for example, a business plan describing efforts to obtain EU customers

Examples of the above may include:

- A single physical location located in the EU
- A website with a country extension (e.g. .uk, .de, .dk)
- A published phone number with an EU country code
- An employee in the EU
- Processing an EU data subject in a CRM, website or Applicant Tracking System
- Accepting payment from an EU citizen
- Shipping product to an EU citizen

Of course, if any of the above situations apply to your company or could trigger exposure to the GDPR, evaluating the "surface area" of that exposure is important to discuss with knowledgeable legal counsel. Remember that there is still much gray area in the GDPR, and regular clarifications to the law continue to be released. It is important to monitor these clarifications closely in order to understand how the GDPR is to be interpreted for your own company.

KEY COMPONENTS AND IMPACTS OF THE REGULATION

The Data Protection Officer (DPO)

Like any change initiative, the first step is to create a sense of urgency. The possibilities of large fines and a concrete launch date should hopefully achieve that. The next step is to identify a "champion" to lead the change. GDPR guidelines actually impose the need for a Data Protection Officer who is responsible for regulatory compliance and reports to the President or CEO. This responsibility can no longer be delegated to a mid-level manager within the IT or data science departments who the CEO can claim was not aware of any shortcomings around data governance. As of May 25th, it is clearly explained that responsibility lies within the C-suite.

It should be noted that the DPO role can be filled by an outside entity. Since qualified DPOs tend to be both expensive and difficult to find, fractional DPOs and DPO-as-a-Service offerings from

professional services companies may be a more viable alternative. Here are some of the main responsibilities of the DPO, as outlined by ITGovernance.co.uk:

- Inform and advise the organization and its employees of their data protection obligations under the GDPR.
- Monitor the organization's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation, and outcomes.
- Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting.
- Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

The DPO's success in achieving these objectives will require support from all levels and functions within the organization, presenting a major opportunity to develop a unification process that transcends silos and builds company-wide efficiencies. This, in turn, could be viewed as one of the first competitive advantages that will be discussed in the next section. It is also important to note that technological solutions exist to support these compliance initiatives.

Data Subject Rights

The most complex requirement in this new regulation is likely Article 17, the data subject's rights, which include the rights to opt-out of processing, view data and understand its use, and to be forgotten (or contest or move data).

At the center of the GDPR is the data subject's right to have visibility into the data any company has tracked or processed for them, as well as how that data is being used by the company. For smaller companies with a single data source like a CRM, this is simpler to address. It may involve development to expose that data to an individual in a way that ensures the person's identity can be validated, the interaction is time-stamped and that these items are demonstrable to third-party auditors and regulators at a later date. For larger companies with multiple data repositories, however, this requirement can be more challenging. Most companies have at least four different

data sources, between CRM, ERP, billing, analytics, human resources, applicant tracking, e-commerce, ticket management, help desk, and websites.

While many companies may be able to handle responding to a few requests manually each month, processing hundreds or even thousands can quickly become overburdening, particularly since the regulation mandates compliance with a request within one month. In these situations, companies will need to investigate solutions for centralizing data and automating the processing of subject access requests and associated individual rights.

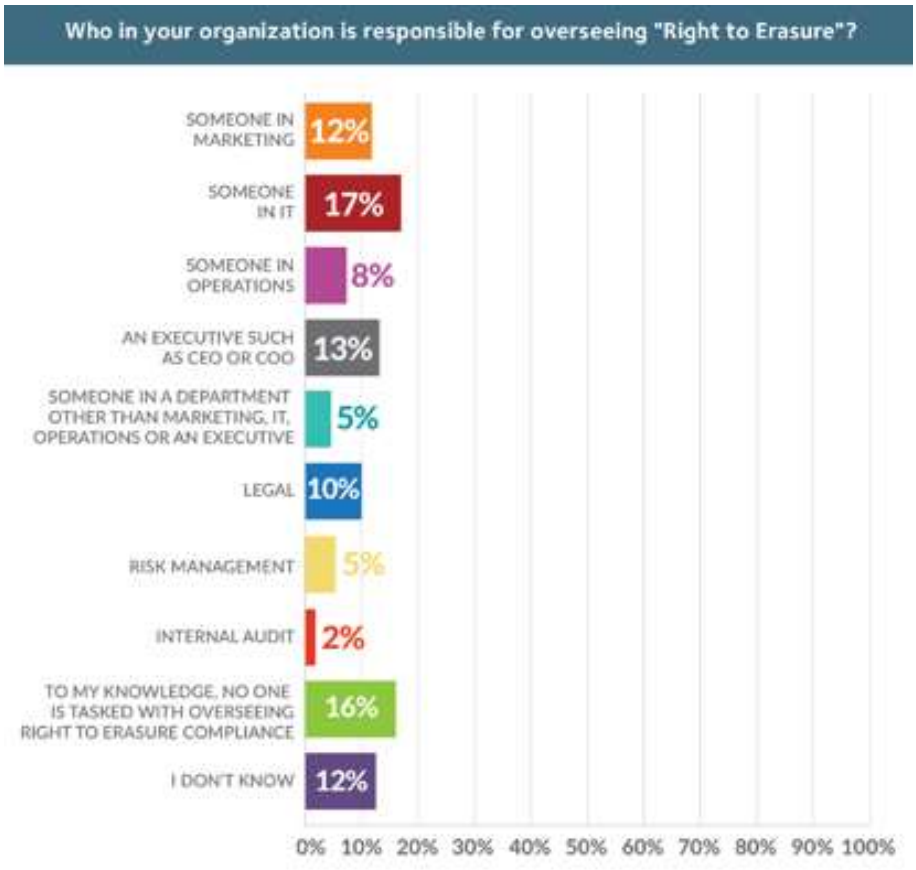
In addition to better visibility, under the GDPR the data subject gains new powers over what can be done with their data. This includes the right to be forgotten and to contest or move data. The right to be forgotten, for example, allows a data subject to request that certain data be deleted, which can include a single data point such as their email address or a particular transaction, or the user's entire data record with a company. From a business standpoint, keep in mind that "forgetting" a data subject does not necessarily mean deleting the record, but in many cases, it involves anonymizing it. Anonymizing effectively removes the data subject's association with a particular transaction, for example, which your business may have a legitimate reason to retain a transaction for proper billing records.

Deleting or anonymizing the data is the easy part, however. Knowing where all the data points are located, and then proving that they have all been deleted, is exponentially more challenging. This is accentuated by the fact that many organizations are unaware of all the past and present data collecting initiatives that various internal departments may have in place. An example of such an initiative might be a special "shadow IT" project whose existence may only be known to a handful of employees. These often circumvent the more formal IT approval processes in favor of speed to market, and are therefore often developed without the full knowledge of the IT department. For instance, a marketing department seeking real-time consumer data might create its own solutions to measure and track customers in its stores. These often run outside of existing IT networks.

Companies must also be aware of—and are somewhat responsible for—their vendors, partners, and third-party software platforms, many of which may be serving as data processors for customer information. Ultimately companies and their vendors share in the GDPR compliance duties, but this does not eliminate an organization's responsibility to ensure those data subjects' rights are properly managed across the data supply chain.

It is also important to note that data subjects' protection rights are not solely applicable to customers. As *David Dadoun, Head of global shoe retailer Aldo Group's Business Intelligence and Data Governance organization*, shared: "...sensitive HR employee data must also be treated with the same care. There is obviously fiscally regulated data such as income tax reporting and the like

that cannot be deleted upon request, but otherwise, employees benefit from many of the data subject privileges as consumers."



Clear Opt-in

When it comes to terms and conditions, consumers click "accept" almost daily while rarely taking the time to read the multiple pages of small print detailing what it is they are accepting. The new regulations demand that the portions of data being collected and the reason behind the collection be written in "clear terms." The GDPR also requires that the option to opt out of communication or processing be just as clear and easy as opting in.

Breach Disclosure

Many data breaches go for weeks, months, or even years before being disclosed. According to a Bitdefender report, the average breach runs over 37.9 days before detection or reporting. Within Article 33 of GDPR, disclosure of a "material breach" to all stakeholders must occur within 72 hours of occurrence - not discovery. This will force organizations to pay much closer attention to breach signals or risk large fines for non-compliance.

Fines that have real impacts on the company's bottom line are intended to instill a heightened sense of urgency and overcome "Breach Fatigue." It seems consumers are becoming so accustomed to data breaches that what used to be outrage (ex. Target 2013 breach) has almost fizzled to indifference. Going forward, when an EU data subject's personal and sensitive data is compromised, apathy should no longer be the typical response.

Compliance with the GDPR will not guarantee a full stop to breaches, particularly as technologies both for attacking and defending databases continue to advance. However, it should greatly boost a company's motivation to respond to breaches in a quick, effective manner.

Automation

Though not explicitly a requirement of the GDPR, the practical effect of all these new elements is the sheer scale at which data discovery, data monitoring, breach management and Subject Access Requests will affect each business. As Chris Babel, CEO of TrustArc said, "The GDPR is driving a fundamental shift in how companies manage privacy. In addition to requiring the development of new processes, companies need to operationalize their program in order to efficiently manage compliance on an ongoing basis. The only way to do this at scale is by using technology to automate the process versus just relying on hiring more people."

For many companies preparing for the GDPR, May 25, 2018 marks the end of the "assessment period" and the beginning of the "operationalizing period" within which platform adoption will likely take center stage.

THE BITE AFTER THE BARK (I.E. THE FINES)

Privacy regulations are by no means a new phenomenon. Most jurisdictions have upheld legislations meant to protect citizens' right to privacy. However, with GDPR fines reaching as high as 4% of global revenues, the repercussions of non-compliance will have substantial impacts on all stakeholders in an organization. In today's hyper-competitive marketplace, 4% can make the difference between a company reporting a profit or a loss, as well as impact senior executive compensation.

The good news is that, as we see it, the opportunities for transparency, trust and business efficiency that GDPR compliance presents should be a far greater motivator than the fear of fines and legal battles.

WHAT IF THE GDPR DOES NOT APPLY TO ME?

Data Privacy and Trust Are Universal

Whether or not a company is legally bound to comply with the GDPR, businesses can still benefit from implementing a solution for transparency, notice and consent around consumer data handling. A company's willingness to take these extra steps will build trust with their consumer base and set them apart from the competition that may be taking a wait-and-see approach. Complying out of duress will be a potential detriment for businesses trying to build a relationship of trust with customers.

Privacy Laws Are Changing Everywhere

The GDPR is currently the most wide-ranging privacy regulation put into practice to date, but it will not be the last. Already, legislation resembling GDPR is being introduced and adopted in Canada, Japan, Australia, and South Korea. Similar legislation is also being introduced in the U.S. at both the state and federal levels. It is only a matter of time before the demands of privacy expand beyond the limits of the EU, and for companies that have already developed the operational and technical infrastructure, those changes will be much easier to accommodate.

ADVANTAGES OF COMPLIANCE

"While compliance is at the core of the GDPR, we are seeing a strong shift toward taking an active posture towards privacy from many leading companies as compliance isn't enough. Consumers today expect to engage a brand on the terms they desire, looking to more deeply engage those companies who are leaders in this area." notes *Ryan Parker, Head of Responsive Retail, Intel Corporation.*

In light of the more recent data and privacy scandals featured in top news stories, we clearly see an opportunity for companies to prioritize transparency as they leverage personal data. Beyond making good business sense, this trust-building exercise demonstrates goodwill, corporate citizenship, and improved brand equity.

Karen Schuler, National Data & Information Governance Leader for BDO USA, stated that the many added benefits of GDPR compliance "would create better business decisions through increases in data quality, integrity, availability and consistency. This could reduce data storage, discovery and knowledge worker costs, driving innovation by delivering higher value data."

Data Mapping

To comply with the GDPR and, in particular, the data subject's right to be forgotten, it's critical to have a comprehensive data map that clearly indicates all data sources, who has access to them, and how they are interlinked and provisioned. The exercise of data mapping, itself, may unlock some unexpected insights into how your organization is structured, which can translate into tangible benefits.

360 View: Consolidate, Understand, Leverage your Data

According to *Ryan Parker from Intel*, GDPR compliance can help your organization gain a better understanding of its customer through a more complete view of the existing diverse data points.

"Customer 360 is all about knowing your customer, who they are, and how they have interacted with your brand. Currently, outside of a few, we still have not seen many retailers develop that 360 perspective because their data is highly dispersed in a host of systems and people. The GDPR could be a great catalyst to finally see all systems come together to provide a holistic picture of the customer's data to ensure compliance. This comprehensive view could finally allow retailers to fully leverage the great business intelligence and artificial intelligence tools that are available on the market today."

Of course, this is all predicated on the consumer. If customers opt out of marketing or processing efforts *en masse*, the ability to understand and predict their behavior will be greatly diminished. It remains to be seen exactly to what level of consumers will proactively exercise their rights under the GDPR, but we can reasonably expect brands to fare better when they act responsibly and create the proper incentives for consumers to both trust and engage.

Impact on Culture, Collaboration & Breaking Silos

We also expect the GDPR to lead to positive impacts on a company's culture. For companies that differentiate through outstanding customer experience, GDPR is a natural progression to better engage the customer in the transparent manner that they expect, thus increasing brand value. For those not yet familiar with GDPR, it is much more than just compliance, it is a new way to engage consumers with their brand through the power of data.

Integrity, Transparency and Trust: Keys to Maintaining Brand Equity

There is a strong correlation between high perceived transparency and positive consumer sentiment. Core brand attributes are most often centered around trust. Building trust with a customer by showing immediate access to their data and providing a rapid response to requests to challenge, delete or move that data, is part of the new definition of trustworthiness. The GDPR has defined this new set of rules for what a trusted relationship should look like, and the early adopters may find a strong competitive advantage through earned trust.

Opportunity to Learn from Emerging Technologies

Like many other new technological revolutions, there are opportunities to understand and master emerging technologies. Some of the more complete solutions leverage the power of both distributed ledger (blockchain) systems and data lake (cloud computing) technologies.

Leverage the Blockchain (Distributed Ledgers)

Aside from the commonly known application of blockchain technology as the platform for cryptocurrency transactions, the cutting-edge technology also holds massive potential to deliver secure encryption and immutability. This ties directly to the needs of GDPR compliance.

As an example, the auditability of GDPR Edge comes from the blockchain ledger where all subject access requests and exercised rights are time-stamped and unable to be altered. Once data from an interaction is gathered, it is transferred to the ledger and then on to the data lake, where all interaction records live. If a consumer makes a request, a detailed record is logged regarding the interaction activity. Once an auditor or regulatory body is comfortable with the system, the lengthy portion of the auditing process can be substantially relieved, focusing instead on the actual results and activities.

Data Lakes & Machine Learning

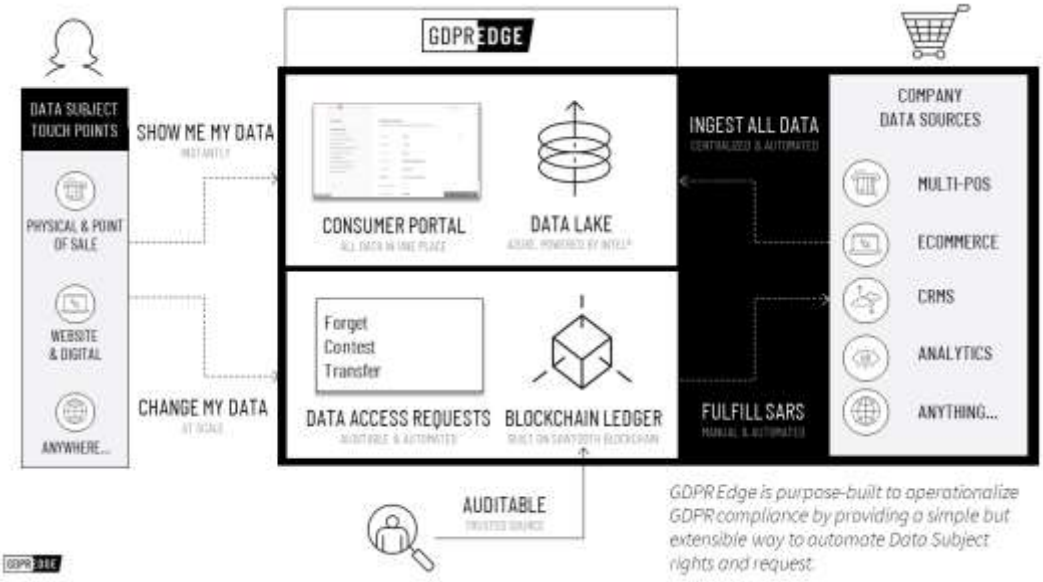
For those companies already focused on centralizing data for GDPR, specifically regarding the opportunities around data lakes, business intelligence, and AI, *Chris Dieringer, National Sales Director at Microsoft - Retail and CPG Industry*, said:

> "*Implementation of a data lake as part of your GDPR strategy acts as a catalyst to increase insight and transparency within the organization. By leveraging a single data lake for GDPR, companies benefit from a single source of truth which can unlock the value of data across their entire business. This approach allows them to find correlations in data that isn't possible when data is siloed, opening new insights and optimizations across the entire company.*
>
> *Additionally, you can leverage machine learning models to find patterns in customer behavior and preferences for better targeted and efficient marketing. You can also leverage the AI platform to engage directly with customers to help them through their journey, while recommending products directly to them and reducing agent cost.*

Of course, to implement such a cross-business data lake, while also enabling Individual Rights under the GDPR, requires that certain data be anonymized and secured, thereby enabling the business without compromising the consumer. With our particular approach to data lakes on the GDPR Edge platform [see below], when you expose your transactions and records to a customer, you can do that in full legal compliance, on our data platform."

GDPR EDGE: AUTOMATING COMPLIANCE

GDPR Edge is a collaboration between BDO USA, LLP and IntraEdge, powered by Intel® Software Guard Extensions (SGX), delivering a blockchain-based solution for the General Data Protection Regulation (GDPR). It brings Blockchain security and data lake architecture to the unique data privacy requirements of the GDPR. Specifically, GDPR Edge allows companies to provide data subjects with the ability instantly see any data a company has tied to them. It also enables an automated and auditable series of events to accept and process requests to forget, contest and transfer that data.

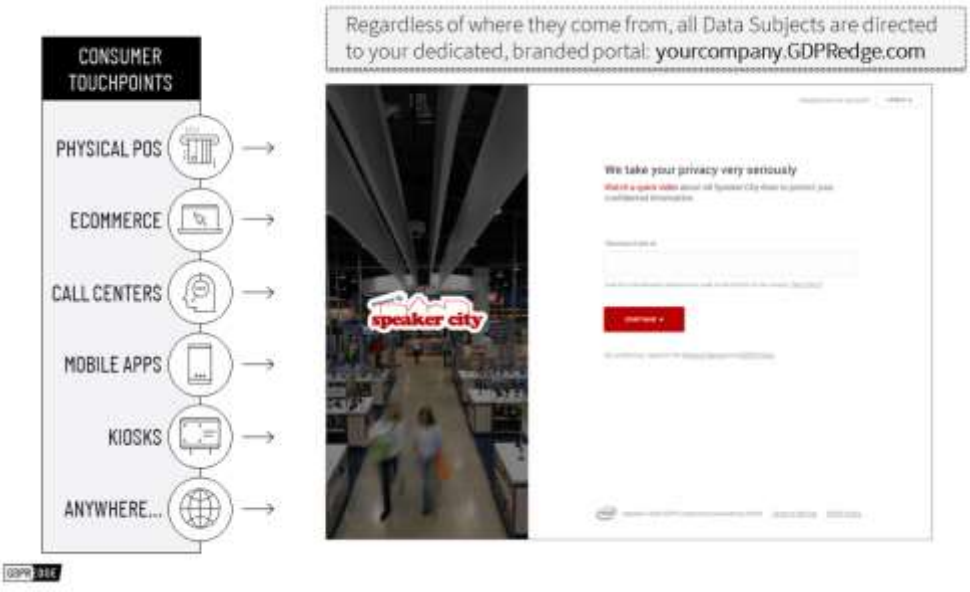


Data Lake at the Core

The GDPR Edge platform accomplishes all of this by ingesting data from any API-driven data source into a centralized data lake, deployed either in a multi-tenant environment or on a company's own cloud or premise environment. GDPR Edge then provides portal views into that data lake for the data subject, the auditor, and a company's own administrators, staff and DPO. Companies can then leverage this data lake as a central repository of all customer data and interaction, opening up the ability to employ modern business intelligence tools to create value where it never existed before.

Visible Compliance: Integration Anywhere Data Is Collected

GDPR Edge also integrates with any interaction point where a company may be collecting information from data subjects. These can include digital interactions through a website, e-commerce, email marketing or mobile apps, as well as physical interaction points such as a physical point-of-sale, kiosk, or trade show interaction. All of these interactions produce data transactions which are fed into the data lake and matched to the appropriate data subject record using easy-to-deploy transaction IDs and direct integration methods. In this way, GDPR Edge enables any company to be visibly and conspicuously compliant with privacy at every interaction.



Secured and Auditable by a Blockchain

Leveraging Hyperledger Sawtooth, GDPR Edge creates a trusted record of all data subject access requests (DSARs), time-stamped and immutable, along with all mitigation steps by a company to fulfill that request. Complete with a workflow engine and straightforward GDPR reporting, GDPR Edge provides an out-of-the-box solution to accept and process DSARs in a way that stands up to third-party scrutiny.

Scalable and Extensible through Automation

For companies that expect only a few DSARs, to those bracing for tens of thousands per year, the GDPR Edge platform can support a largely manual effort or fully automate your DSAR mitigation operations. With automation available natively in the platform and through APIs to unlimited back end systems, GDPR Edge can grow with any company as its policies and needs change over time.

Implement in Days and Automate Over Time

The GDPR Edge platform has flexible implementation options. Many companies have complex long-term system requirements but relatively simple needs in the short-term. GDPR Edge allows any company to activate the platform within days, enabling fast access to visible and conspicuous compliance. A quick-start implementation may include a single system integration paired with some manual workflows but still brings the immediate power of all the ledger, task management and reporting elements of the solution.

GDPR Edge is both a powerful solution that proficiently serves complex organizations and an easily implemented alternative to manual DSAR processes; enabling companies to quickly demonstrate their compliance and automate the ongoing impact of the GDPR access requests.

To learn more about GDPR Edge, An Intel ® IoT Market Ready Solution, and how this technology can support your business with GDPR compliance, visit gdpredge.com.