GDPR: Risk, Revenue and Reward

Risk is only one part of the equation when it comes to the impact of the GDPR. The other important "R" to watch – is its upcoming impact to your Revenue. Learn the key considerations that can allow your business to close both risk and revenue gaps, at the very same time.

A PEGA WHITEPAPER

PEGA

Build for Change®

Introduction

According to a Q4 2017 Pega survey, consumers state that once they are made aware of the upcoming General Data Protection Regulation (GDPR) legislation, the vast majority (82 percent of EU resident respondents) state that they are likely (51 percent), or highly likely (31 percent), to exercise their rights. Only 10 percent said that they were not likely to do so. This has many businesses rightfully asking – are we going to be ready for the arrival of GDPR? And what does it really mean to be ready?

All the world is talking about the GDPR and its impact to compliance and risk. But there is a major misconception – that the legislation is solely about risk. And this misconception is one that will catch many businesses flat-footed if they don't have the right strategy in place.

The reality is that the GDPR represents much more than just a risk issue. Risk is just a piece of the upcoming legislation's likely impact to your business. There is an important second "R" that must be addressed – revenue.

As we will share, your business will need to have six core competencies firmly in place around GDPR personal data profiling, processing, and automated decisioning provisions to close gaps for risk-readiness. You will also need to have two new superpowers when it comes to your strategy to maintain or extend your position when it comes to revenue-readiness. And if you plan your strategy right, you can close all of these gaps with the very same budget.

Achieving risk-readiness: The 6 critical capabilities for GDPR compliance

At its core, the GDPR is a challenge of orchestration. And many are waking up to the reality that in order to comply, it's not a question of if you have "a system" to manage the GDPR – it's whether you have **a system to manage the systems** – that you'll need to comply with the GDPR.

Let's take a look at the six core capabilities that are key to closing the gaps for your GDPR personal data profiling compliance strategy. These capabilities fall under the following headings: consent, process, data, communication, insight, and accountability.

1. Consent

Your business must build a competent procedure for the collection and maintenance of continuous consent with each EU data subject. This consent is not a one-time action. It must become an ongoing activity for your business.

The initial collection of permission and preference is just the commencement of this process. And many steps must be taken. For most, this will include the confirmation – or proof – of the agreement to consent to the use of the data provided, and for which purpose. Best practice should also include the proof of the specific terms of consent that were presented to the data subject at the time of collection. In some cases, businesses, including your own, may make an argument of "legitimate interest" as a substitute for explicit consent.

Importantly, once collected or declared, data subject consent will need to be continuously governed and administered across

your business' systems and processes, in accordance with the permissions (or legitimate interests) granted. In this sense, it will be as much about what your company doesn't do, as well as what it does, when it comes to future customer profiling activities and interactions.

Enabling technology for GDPR consent compliance

Due to the nature of permissions, preferences, proof, and governance that will need to be administered at the individual level, the use of a centralized context broker, or decision hub strategy will be central to success. This consent is much more than your marketing preference center of today. Its function must be universal, accounting for the permissions to use each individual's data – not just for marketing offers, but sales, service and even operational functions.

And it should apply to the consent of channel use, by function. For example, some communications such as potential fraud may be welcomed via SMS, while others such as marketing offers may be restricted to email.

Once configured, your solution can then facilitate a centralized authority for a customer's state of consent, across all future decisions made by your business

2. Process

GDPR's orchestration challenge centers upon establishing new closed-loop processes that in most cases, will not exist today. It's not just a matter of having the consent, or knowledge of data sources. It's about "the how" of getting compliance done – how you will initiate, automate, track, and report on each and every GDPR event, everywhere across your enterprise.

Most businesses are planning to begin their compliance journey with a mixture of manual and automated processes, and a plan to automate as much as possible, as quickly as possible, over time. The problem is that these processes don't happen by themselves. And they won't happen in a compliant manner at scale. In fact, every manual process serves to open your business up to GDPR risk exposure for gaps in compliance, accuracy, and audit trail.

Manual processes also expose your business to compliance risk when it comes to the legislation's provisions around security and encryption (Article 32, Security of Processing). Best practice will entail protecting a data subject's personal level data from the moment it is collected, through the moment it is accessed under the GDPR.

Enabling technology for GDPR process compliance

In short, your business will need to interpret the GDPR legislation and establish its

own position regarding the mandate's articles. Whatever the interpretation, the next challenge is to make sure the rules are followed. For this reason, from the commencement of your GDPR compliance journey, a best practice should be that even your manual processes are governed using "dynamic case management" technology.

Employing dynamic case management, your business can rapidly configure how your process should flow, and establish the supporting workflows that can turn it into a reality – without software coding. This strategy provides the material evidence the governing body will demand of your business' processes, the steps you have taken, and assurances of adherence to your protocol. Another major benefit to this approach is that it allows the business to add-in automations over time, via APIs, and robotic automation, while leaving the process itself in place and intact.

And when it comes to understanding which manual GDPR processes to automate with the greatest urgency, a technology called Workforce Intelligence may be employed. This form of analytics installs on your workers' desktops, and quickly automatically quantifies the top opportunities for automation.

3. Data

One of the first steps in beginning your path toward GDPR data compliance is to discover and identify, as a business, all the places where individual level customer data may be residing across your enterprise. In addition to the master data management (MDM) efforts that your business likely has under way, you will need to provide a new capability to collect and assemble this data – on demand – when a GDPR event, such as an Article 15 data subject access request, is initiated.

This is no small task. Consider that most businesses have had "360 degree customer view" initiatives that aspire to serve up a complete record of customer data to frontline employees and internal systems – and it is still not a reality for many brands. Now, with the GDPR, your business will be tasked, for the very first time, to assemble this 360 degree customer view, but to give it directly to the customer. The tables have turned, and now there's a deadline (May 25, 2018).

Enabling technology for GDPR data compliance

To close this gap of GDPR orchestration, your new challenge will be multifaceted. You will need to establish new processes, both where APIs exist and even where they don't.

Yes, that old mainframe where you still keep customer data, that doesn't connect to anything, will still need to play a role in your GDPR compliance strategy. Will you have employees manually look up data and enter it into other screens by hand? For some, that's the current plan. But there's a more effective way, which is also less risky.

a. **Where API's may exist –** Solutions such as Pega's Integration Wizards, simplify the process of integrating with API-based data sources, guiding your administrators through the process of defining the data model from a WSDL, for example XML/JSON. Standard integration connectors are also available for SOAP, REST, and other integrations.

b. **Where they don't –** Unfortunately, not every GDPR impacted system will have a clean API or easy integration, presenting a major challenge for compliance. Rather than leave this to time-consuming, expensive, and error- prone manual data query and duplication, best practice should be to employ robotic automation technology. A fast fix, these "software robots" can function both at the desktop level, and "headless" intersystem level. This breakthrough allows you to distribute work across desktops, employees, and servers, so you can scale to meet your GDPR compliance needs. This is done without replacing existing systems or forcing additional workloads upon employees.

A final best practice will leverage a system of data abstraction that separates the "ask" of the data, from the data itself. Pega calls this the concept of "live data." This ability connects to your MDM solution, or data repositories, directly whenever data must be pulled or pushed, all while maintaining a rich audit trail of its activities. And while doing so, Pega can provide extremely secure encryption capabilities, as you must take steps to protect and encrypt the customer level data at every step during this process. This includes both when your data is at rest and when it is in motion, even within your own GDPR procedures.

4. Communication

A system of orchestrated communication must also be established as part of your framework. This includes the ability to, at a minimum, govern the communication between your business and each data subject for the following critical aspects:

a. **Identity confirmation**

b. **Breach notifications**

c. **Consent expiry**

d. **Policy changes**

When it comes to ensuring each data subject's identity, the stakes are incredibly high. Even individuals whom are authenticated in one's online website may pose risk. Consider that there is often a great deal of sensitive personal data that is not typically served up into account access screens, including citizenship data, answers to personal security questions, and much, much more. To a hacker that has cracked the simple password they forgot to change, it can be just a few clicks to log in, change the email address on record, and fraudulently request a copy of all of another person's data. For this reason, many are advising that any change to customer data (rectification), request for access, erasure, or any other GDPR challenge be subject to a double opt-in style identity confirmation.

Enabling technology for communication compliance

Your communication orchestration may not be as simple as integrating into a marketing email service provider (ESP), or firing off manual emails from your Outlook client. It must be automated, ironclad, and lock-step with your closed-loop processes. It must accommodate functioning both in batch, and individually.

It must be tracked from end-to-end, including the ability not just to send, but to await and accept responses. In its most basic form, this may include single-click responses, such as in the process of identity confirmation.

In more troublesome examples for your business, this can include more complex scenarios such as a manual email in the form of unstructured text. Technologies such as Pega's Intelligent Virtual Assistant for Email, can automate these interactions, by applying natural language processing (NLP) and instantly understanding the intent of the communication, any applicable open cases, and automating the assignment. And to solve the challenge of your master communication orchestration, across batch and individual interactions, the deep capabilities within sophisticated applications such as Pega Marketing and Pega Customer Decision Hub may be employed to link seamlessly with process orchestration.

5. Insight

Many businesses will also be directly impacted by the GDPR's articles pertaining to automated decision-making, such as the mainstream approaches of "real-time decisioning" and AI applications (articles 13, 14, 15, and 22). Each data subject will now have the ability to restrict this form of processing, in particular, where the decision "produces legal effects concerning him or her or similarly significantly affects him or her" (article 22).

The key to this aspect of the legislation is not just permission, but transparency. Industries such as finance, healthcare, and insurance will feel it most.

In particular, businesses could be on the hook to explain and share "meaningful information about the logic involved" in making affected automated decisions.

For this reason, if your business relies upon "black box", or opaque analytic techniques, such as deep learning, you may need to quickly find alternative methods, as well as a means of governing where and when these types of opaque techniques are (and are not) permitted. And you'll have to prove it, as individuals will have the new right to object and question any decisions made – for example, questioning why a loan application was rejected, or a higher interest rate was offered than the one advertised. It likely won't be enough to simply show the data used by the logic and call it a day. If you used an AI algorithm, it'll need to be explainable.

Enabling technology for insight compliance

To achieve compliance for automated decisioning, a new level of transparency is required. If your business is impacted for certain types of decisions, it will now need to apply transparent AI strategies, rather than opaque, so that the logic of the decision made may be better interpreted and understood. And it's not just a matter of seeking out alternative decisioning approaches for these use cases – it's also about ensuring that the dangerous opaque techniques are not accidentially applied.

For this reason, Pega has innovated the industry's first "T-Switch" (T for "Transparent" and "Trust") to empower your business to selectively regulate where and when these varying levels of transparent, or opaque, AI may and may not be used – and for which use cases. This T-Switch comes as a standard component of Pega® Customer Decision Hub .

6. Accountability

The bottom line when it comes to all things GDPR? Prove it. It's not just about the execution. It's about providing evidence of compliance to each of the GDPR's challenging articles.

Which steps have you taken? How exactly did you provide each data subject the resolution they demanded? How long did it take? How did you validate each data subject's identity at the time of the GDPR request? Which safeguards did you put in place while their data was in motion?

And, again, when it comes to automated decision-making, you could also be on the hook to provide evidence of not just the decisions that were made, but also how they were made.

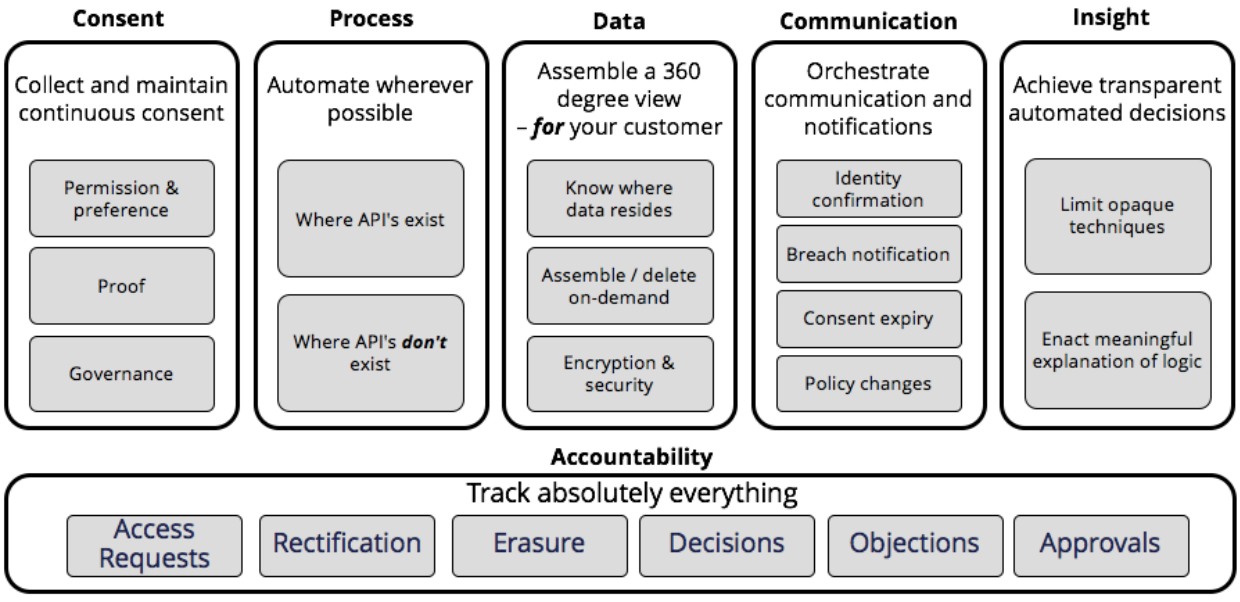
Enabling technology for GDPR accountability compliance

Your accountability strategy cannot be an afterthought. It has to be in the very bedrock of your processes. Pega solutions include the out-of-the-box ability to track everything, across each of your data movements and GDPR processes. With extensive logging and tracking, this includes your ability to play back not only which interactions occurred, and the automated decisions made along the way, but also the customer data that supported those decisions at each step.

And, for additional granularity, capabilities such as Pega® Business Intelligence Exchange (BIX) can provide the ability to automate the selection and extraction of data into external files (in XML or comma-delimited format), or a relational database.

By incorporating these six core capabilities of consent, process, data, communication, insight, and accountability into a holistic strategy, your business can establish "the system to manage the systems" to close your GDPR compliance gaps.

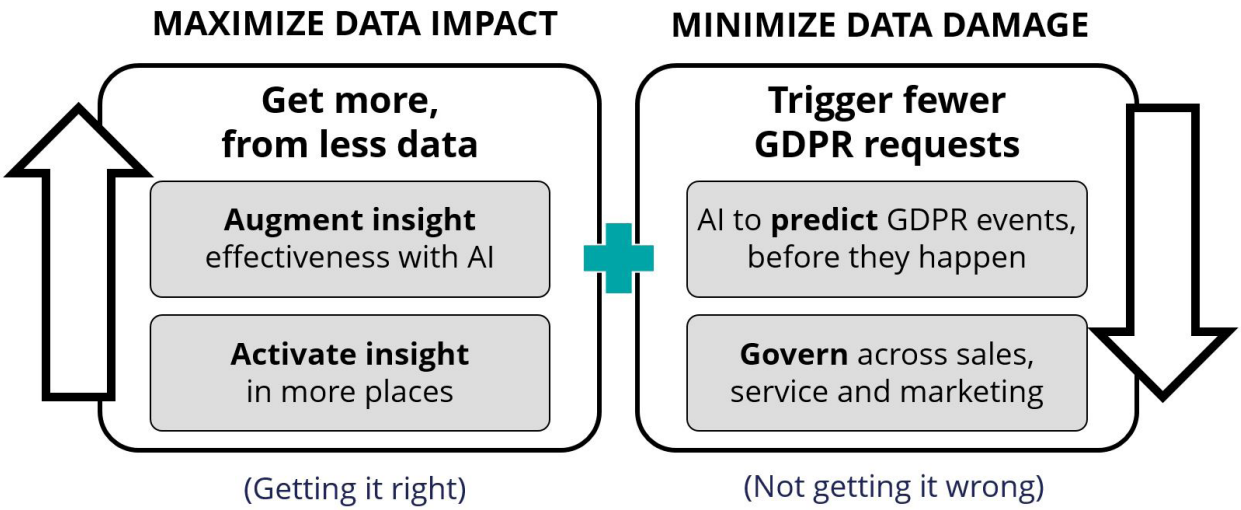
Illustration: The six core competencies for GDPR risk-readiness



Achieving revenue-readiness: The GDPR's looming impact to your bottom line

Many have mistaken GDPR to be simply an issue of compliance or risk. The wake-up call comes when businesses finally look close enough to realize that GDPR legislation is not just a problem of risk – but of revenue. And it is much more than the potential 4 percent fine that comes with failure to comply.

Your revenue exposure will fall into two categories:



1. Getting it right: Extracting greater results from less customer data

Consider that for more than a decade, the thirst for data-driven decisions has exploded. Businesses of all shapes and sizes have established proficient practices that dissect and analyze customer data, for the purpose of understanding customers better and to influence customer lifetime value (CLV).

Of course, the fuel for any business' insight engine is customer data. Over the years, you've acquired customer data not just from individuals, but also from third parties, in the hope of gleaning greater insight into each individual's needs and behaviors.

Now, a new reality is about to sink in: Beginning May 2018, each business will not have more customer data to work with than today, but in all likelihood, less. And with less customer data to work with, the new reality becomes that businesses will need to improve their insight-driven practices, and achieve greater accuracy to produce the same results of today.

This will mean a new requirement to use the customer data you actually do have, to its absolutely greatest potential, using more insight, in more places than ever before.

2. Not getting it wrong: Limiting the triggering of GDPR requests

But it's not just that you'll have to get better at getting it right. You'll also have to develop a brand-new competency around making sure you don't get it wrong. Indeed, every "less-relevant" interaction brings your organization one step closer to a GDPR-driven complaint. According to the Q4 2017 Pega GDPR Consumer Survey robocalls, irrelevant marketing, high marketing frequency and poor customer service interactions are among the likely triggers for initiating a GDPR process with your brand.

Interactions such as these, lead an individual to question why they have been treated in a certain way (sales, service, and especially marketing), and will only increase the probability of a data access or erasure challenge. It will most often be your own actions as a business that will drive the data depletion – and costs – that come with each GDPR-driven event.

The problem is that until now, marketing offers have been largely regarded by marketers on a scale of being either highly relevant, or potentially relevant, with degrees of difference in-between. Any given offer could hold the opportunity to drive revenue, so very little marketing has been held back. Consider that the average marketing campaign yields just a 1-2 percent response rate (hint: that's a 98-99 percent failure rate).

Come GDPR, the next best action at any given moment in time, may be to do nothing at all. The businesses that will best rise to the challenge will reframe this definition, and put in place new processes to ensure that potentially irrelevant content and treatments are instead held back – not just in batch – but in real time.

These two aspects of augmenting insight effectiveness, while at the same time restricting communications, may seem to be at odds with each other. They will, however, become critical elements of your new strategy on your road to revenue success in the era of GDPR.

Enabling technology for GDPR revenue-readiness

The key for GDPR revenue-readiness will lie in the decisions that you make. The relief comes when you realize that, if you devise your strategy effectively, the very same technology that you put in place to mitigate your GDPR risk-readiness may also be used to address GDPR revenue-readiness. Quite literally, the same budget that your business allocates for vanilla compliance, may be used not just to close your revenue gaps, but exceed them.

To this end, Pega software features the industry's most powerful AI-driven analytics for arbitrating the next best action, for every individual – in real time. It understands CLV, the risk and the reward of every action and potential action, and making the most of the data you have. And of course, it works seamlessly with all of the existing infrastructure you already own today.

Conclusion: Risk, revenue, and reward

GDPR is coming. For those businesses that can devise an effective strategy for both risk and revenue readiness, there can be great reward. While your competitors may miss the golden opportunity, and devote their efforts (and budget) into systems that can only assist with compliance, your business can use this moment as an opportunity to cattipult past them. This is achieved not just by solving one of these orchestration challenges, but both, from the very same infrastructure – if your requirements are set right.

Keep these two "R's" of risk and revenue in mind as you prepare your strategy for success. If you do, the rewards will follow.

ABOUT PEGASYSTEMS

We are Pegasystems, the leader in software for customer engagement and operational excellence. Our adaptive, cloud-architected software – built on the unified Pega® Platform – empowers people to rapidly deploy, and easily extend and change applications to meet strategic business needs. Over our 30-year history, we've delivered award-winning capabilities in CRM and BPM, powered by advanced artificial intelligence and robotic automation, to help the world's leading brands achieve breakthrough results.

For more information, please visit us at **WWW.PEGA.COM**