Taking on General Data Protection Regulation (GDPR)

Implications to processing, profiling and communication compliance

A PEGA WHITEPAPER

PEGA®

Build for Change®

GDPR basics

GDPR is coming. Are you ready?

The European Union's General Data Protection Regulation (GDPR) legislation **goes into effect May 25, 2018,** with major repercussions for global businesses in terms of how they collect, process, and store customer data. This is more than a compliance issue – it fundamentally changes how businesses operate. Furthermore, the GDPR doesn't just apply to European companies – it affects every international business that handles data belonging to EU residents. Your organization could be fined up to 4 percent of global revenue if you don't comply with GDPR mandates. So, if GDPR compliance is not a top priority for your company, it's time to rethink your approach.

"Push privacy and GDPR to the top of your organization's priority list."
-Forrester Research[1]

Over half of U.S. multinational companies say GDPR is their top data-protection priority. A recent PWC survey uncovered that 92 percent of respondents viewed GDPR as a top priority – with more than half indicating that GDPR readiness is the absolute highest priority for their data and security strategy.

Even outside the EU, sizable budgets are being allocated to ensure companies close this gap. According to this same PWC study, 68 percent of U.S. multinationals stated they will invest between $1 million and $10 million to take on GDPR. And nearly 1 in 10 businesses (9%) expect to allocate more than $10 million to the challenge.

What's all the hype about?

It is a fundamental shift. Until now, an individual's data that a business possessed has been largely regarded as belonging to the business: This is about to change. Soon, any personal level data pertaining to an EU resident will be legally regarded as that individual's personal property, with the individual retaining a multitude of rights relating to their data that is held by businesses across the globe.

As of May 26, 2018, if an EU resident requests to see all the personal data you have on them, you will be legally compelled to comply. In essence, you will have to be able to assemble a 360 degree view, not just *of* your customer, but *for* your customer. Your organization will need to have the systems and processes in place to make it happen. It's irrelevant if you have umpteenth data silos and a lengthy list of disjointed legacy systems that don't talk to each other – you will be expected to respond to an individual's request for their data within a relatively short time – a month, to be precise.

Furthermore, you will only be able to use each customer's personal data for the reasons for which they provide consent. And, according to GDPR Article 7, "consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."

The legislation covers not just the communication of data that the individual has provided to you, but even personal data which has been *acquired elsewhere* (Articles 12-14), as well as all the associated processing and profiling your business may be performing.

[1] Source: "Identify Companywide Roles And Responsibilities To Support Your GDPR Compliance Efforts," June 20, 2017, Forrester Research, Inc.

Key definitions: personal data, processing, and profiling

Here are some of the key definitions that are most important to understand when it comes to the implications of the introduction of GDPR, as stated in Article 4 of the legislation itself.

Table 1. GDPR definitions

Term	Definition	Examples
Personal data	"Any information relating to an **identified or identifiable natural person** ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."	*Data including name, address, age, income, eye color, user ID, twitter handle, email address and other such personally attributed data.*
Processing	"Any operation or set of operations which is **performed on personal data** or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."	*The capture of personal data on your business web site or via paper form, saving one's personal data to your system of record, or performing ETL processes upon those data.*
Profiling	"Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."	*The profiling of personal data for marketing segmentation, and eligibility for product or service offerings.*

Key points of the legislation: process, profiling, and communication

Between now and May 2018, your business will need to obtain specific permissions to process and profile personal data. This will often mean re-engaging with any affected EU resident and obtaining their consent to possess and utilize their data, along with outlining the intended purpose, time period for storage, location of processing, potential for automated decisioning, and more.

The impact of GDPR begins from the very moment personal data is solicited and collected (Articles 12-14), regardless of whether that data is sourced from the individual directly or via an external source.

The GDPR articles that will most likely impact your business are as follows:

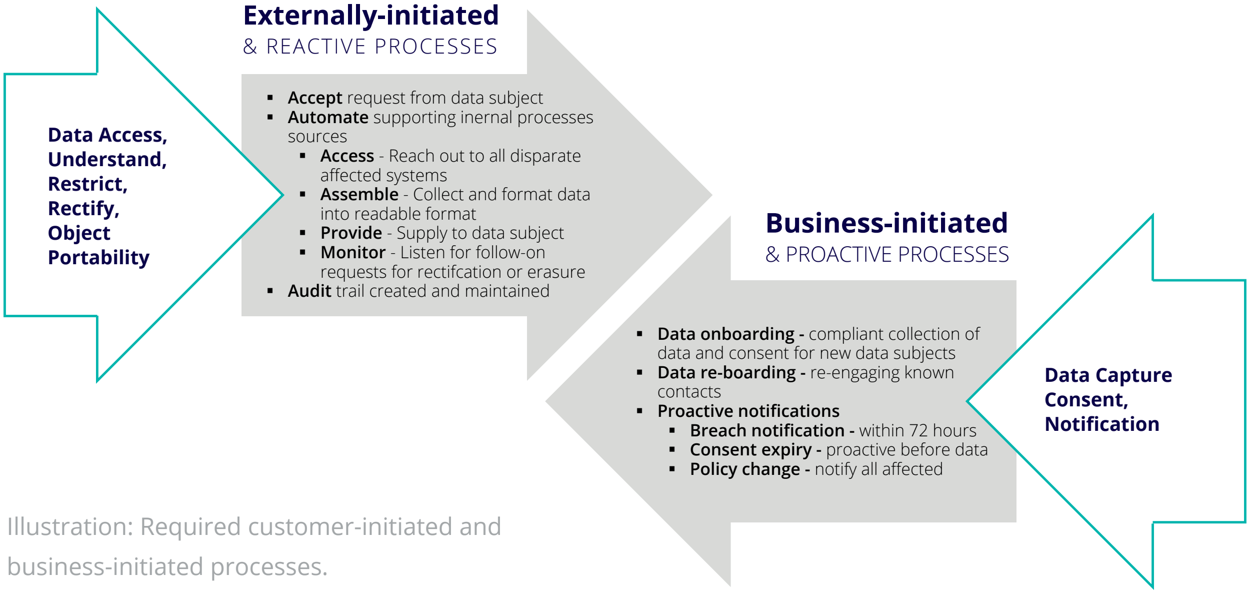
Table: Articles pertaining most to personal data and processing.

Articles	Short Description
Right to Access (Article 15)	The right of EU residents to demand visibility and access into any personal data you may have.
Right to Rectification (Article 16)	The right of EU residents to correct or change any of their personal data that you may possess.
Right to Erasure (Article 17)	The right of EU residents to demand permanent erasure of any, or all, of their personal data.
Right to Restriction of Processing (Article 18)	The right of EU residents to permit, and limit, the processing of their personal data.
Notification Obligation (Article 19)	The mandate that a business must communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18.
Right to Portability (Article 20)	The right of EU residents to receive one's personal data in a structured, commonly used and machine-readable format, as well as the right to transmit the data to another controller.
Right to Object (Article 21)	The right of EU residents to object to the processing and/or profiling of one's personal data.
Automated individual decision-making, including profiling (Article 22)	The right of EU residents not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly impacts the individual.
Records of Processing Activities (Article 30)	The logging and auditability of the processing which has occurred including the purpose, categories, recipients, time periods, and more.
Security of Processing (Article 32)	The pseudonymisation and encryption of personal data, including maintaining the confidentiality, integrity, availability, and resilience of processing systems and services.
Notification of a personal data breach (Article 33, 34)	Communication of any data breach to multiple parties, including at minimum, the data subject and supervisory authority.

Note that this represents a summary list of article highlights only. Pega highly recommends your compliance team read the full contents of all GDPR articles in their entirety before forming the basis of their full GDPR strategy.

Articles 15-22 must be performed "without undue delay and in any event within one month of receipt of the request" (Article 12). Consequently, it's important to devise strategies to automate workflows as much as possible across all processes.

Notably, the provisions within these articles describe a two-way street. Your business will need the ability to react to external requests, and you'll need a host of business-initiated and proactive processes as well.



Externally-initiated
& REACTIVE PROCESSES

Data Access, Understand, Restrict, Rectify, Object Portability

- **Accept** request from data subject
- **Automate** supporting inernal processes sources
  - **Access** - Reach out to all disparate affected systems
  - **Assemble** - Collect and format data into readable format
  - **Provide** - Supply to data subject
  - **Monitor** - Listen for follow-on requests for rectifcation or erasure
- **Audit** trail created and maintained

Business-initiated
& PROACTIVE PROCESSES

Data Capture Consent, Notification

- **Data onboarding -** compliant collection of data and consent for new data subjects
- **Data re-boarding -** re-engaging known contacts
- **Proactive notifications**
  - **Breach notification -** within 72 hours
  - **Consent expiry -** proactive before data
  - **Policy change -** notify all affected

Illustration: Required customer-initiated and business-initiated processes.

GDPR and automated decision-making

Additionally, many businesses are quickly discovering that they will be directly impacted by GDPR's articles pertaining to automated decision-making (including articles 13,14,15, and 22). Industries such as finance, healthcare, and insurance will feel it most.

The key to this aspect of the legislation is not just permission – but transparency. As detailed in article 22, individuals will now have the ability to restrict this form of processing *"the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."*

And even when individuals provide consent to automated decision-making, businesses will be on the hook to explain and share "meaningful information about the logic involved" in making those decisions.

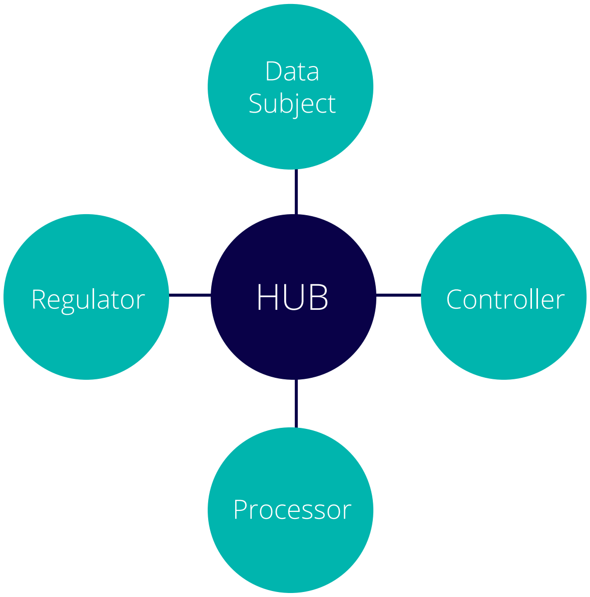
For this reason, if your business relies upon "black box", or opaque analytic techniques, such as deep learning, you may need to stop and find alternative methods, as well as a means of governing where and when these types of opaque techniques are – and are not – permitted.

The REAL challenge of the GDPR puzzle

The question isn't if you have the system to handle GDPR. It's whether you have the system, to manage the systems, to handle GDPR. It's about end-to-end orchestration, governance, dynamic processes, and auditability. It's about getting your old systems to work with your new systems. And your really old systems to work with your next systems.

This orchestration doesn't exclusively involve the data subject – four primary parties are involved in the communication flow.

- Data Subject
- Controller
- Processor
- Regulator



Customer engagement implications of GDPR

Implications to customer service

To avoid major fines and mistrust among their customers, contact centers of all sizes will be forced to rethink their current standards around data protection and privacy with GDPR compliance. Given the enormous amounts of contact information, data, and communication channels accessed and stored to deliver 24x7x365 personalized customer service, **the contact center could be the most susceptible touchpoint for data privacy fraud.**

Need proof? Consider all the customer service channels and options that exist in a contact center today – this could be phone, chat, email, co-browse, social. And then consider how these are used across live agent service, assisted service, and self-service. It's a very wide communication map full of potential risks – especially considering that customer service agents still write down sensitive data like account information, social security numbers, telephone numbers on post it notes, and leave it on their desks at all times.

Similar to the impact that the Payment Card Industry Data Security Standards (PCI-DSS) compliance had on US-based contact centers, being GDPR compliant will provide much more scrutiny on how that information is accessed, processed, and stored across multiple channels – whether it's a name, address, IP address, or telephone number. Since larger contact centers involve a lot of moving parts, employing new and outsourced agents, it's also critical to understand how and where agents are accepting information from customers to ensure full GDPR compliance. Believe it or not, this could include providing your online chat logs and much more for data access requests.

To be ahead of the curve, assess your current contact center capabilities for GDPR compliance requirements now, as this will most likely require a full audit of all interaction flows, infrastructure, and current processes used. This will provide a much better understanding on what needs to change so that your agents are well versed on the implications of data security and privacy.

Implications to marketing

Because of the scale, speed, and scope of its programs, marketing introduces some of the most complex (and potentially risky) GDPR implications. With data from across the organization utilized for inbound and outbound programs, across both owned and paid channels, marketing touches customers more often, and in more ways, than any other business function. It has become the "face" of an organization – which is a double-edged sword. Great marketing can bring customers closer, and enhance the customer-brand relationship. Bad marketing, however, has the opposite (and immediate) effect. Consumers have an extremely low tolerance for any messaging they consider creepy, or overly "salesy."

Any touch that isn't relevant, timely, contextual, and consistent is likely to interrupt and distract from their experience, rather than enhance it. And such interruptions inevitably lead to GDPR-oriented questions such as "How do they know that? What data do they have? How are they using it? Is my privacy safe?" Bad marketing, in other words, can cost you both data, and money (to service customers GDPR concerns), while increasing exposure and risk.

Need proof? Consider all the marketing channels utilized by a typical program, today – email, web, search, mobile, SMS, digital ads, direct mail, outbound calling, etc … and then consider the inside-out, sales-driven way that campaigns are designed. Ponder the loose-fitting, "touch as many people as we can" methodology typically used for audience targeting. Think about how specific customer messages and channel selections are determined by practitioners, often using anecdotal evidence, basic aggregations of click-through rates, and broad-based segmentations. Then consider how often data may be extracted and compiled by hand, and then distributed to partners throughout the advertising technology ecosystem via email or FTP. Each of these scenarios puts a brand at major risk – of breach, service costs, brand damage, and more.

Beyond the impact of the U.S. CAN-SPAM Rule and National Do Not Call Registry, or the EU's ePrivacy Directive, achieving and maintaining GDPR compliance will require a *much higher degree* of scrutiny around how customer information can be accessed, processed, stored, and retrieved across multiple channels. Another consideration is whether the contact information used to match and link different sources (or to distribute through channels) contains data like names, addresses, emails, social handles, IP addresses, or telephone numbers and product names, among other things. Given that large marketing programs often have 25 or more components within their marketing stack, they *already* have lot of moving parts – so it's critical to understand how those data sources and distribution channels can be adapted to align with regulations, and stay in GDPR compliance.

To stay ahead of the curve, assess your current marketing capabilities for GDPR compliance requirements now, as this will most likely require an audit of your data, access rights, interaction flows, infrastructure, software components, and the supporting processes. This type of assessment will provide a much better understanding of what needs to *change,* so that your teams are well versed on the implications of data security, and how they will need to adapt to keep the organization compliant.

Implications to sales functions

There is good news and bad news for sales executives when it comes to GDPR implications. First, the good news. Because GDPR does not restrict inbound sales contact, such as website, telesales, or even social media contact, you can still live chat, call, and Tweet with as many prospects as you wish. But the moment personal data is collected during these interactions, you're on the hook. As well, events and other forms of lead generation – as long as opt-in permission is granted – are OK because the prospective client is expressing interest in your products and services.

Now for the bad news. With opt-in lists getting smaller, you're going to have a smaller pool of prospects. As such, sellers need to work closely with marketing who are more adept at managing quantities of leads and the associated permissions.

Importantly, businesses should begin to expect data access requests – even during sales interactions. This will mean enabling front line sellers to accept and initiate these requests. And don't forget that as your sales staff begin to collect personal customer data, there will be a new variety of permissions and disclosures that must also be presented.

Privacy by Design (Article 25)

Another significant impact of GDPR lies in its principle of "privacy by design." Specifically, once GDPR takes effect in May, 2018, Article 25 outlines that among other conditions, as any new system is designed, "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." What this means is that any organization that establishes a new set of processes or infrastructure must have GDPR compliance in its core plan, no longer as an afterthought or add-on.

7 steps to GDPR success

Taking on GDPR will involve the establishment of an entirely new set of processes that likely go far beyond your current consent and preference capabilities. Here are some of the minimum core implications your company will need to consider:

1. Document your current and future state

This will allow you to produce the evidence that is required by the legislation, as well as uncover any potential gaps in process and technology.

2. Establish new closed-loop processes

Any process for consent that involves manual steps will expose your business to a potential risk in compliance. Consequently, you need new closed-loop processes that are dynamic and able to adjust to the nuances of each request. This includes the capturing and governance of consent, as well as the downstream processes to support the GDPR's many articles - from access, to erasure, restriction, rectification and beyond.

3. Connect disparate data sources

You need to find a way to connect the processes to customer data and systems throughout the enterprise. Importantly, this often include the need to integrate with dated legacy systems that may not have API's.

4. Enact protections for customer data

You must put safeguards in place to proactively protect personal data. This means considerations for encryption, de-identifiction and phseudonymization of data.

5. Create a system of notifications

You need to automate communication across all parties, including the data subject, the controller, processor, and the regulator – with both proactive and reactive processes, including the assembly of dynamic content.

6. Achieve transparency in automated decisions

You may need to cease opaque analytic processes, and replace them with transparent processes that can shed light into the logic used in making the decision.

7. Maintain comprehensive audit trail

You must track all activities, including the capture of data, the granting of consent, and even the decisions that have been made using that data.

Pega makes post-GDPR leadership possible…today

GDPR and customer engagement – much more than a compliance issue

GDPR isn't just a compliance issue – it is also a customer engagement concern with the ability to impact both a consumer's experience as well as your business' bottom line. With these new rights, customers are not just empowered to administer preferences, but also understand exactly how you're using their data and for what purposes.

And when it comes to these purposes, your business will no longer have free reign to repurpose data that has been collected for other reasons. This directly impacts your organization's ability to leverage any customer level data you collect – and even the data you have already collected – for the purpose of profiling and direct marketing.

The challenge doesn't end once you have all your permissions in place. You need to establish a system of governance to make sure the permissions are enforced. Furthermore, each interaction with your customer will come with an additional set of considerations, as every conversation presents a real chance that an individual will seek to question the terms of their relationship with your company and withdraw their data and consent.

How to make GDPR a golden opportunity

Don't mistake this moment. The brands that will win are the ones that view GDPR not as a compliance issue, but as a golden opportunity. Your budget is being developed to fund the key infrastructure needed to support GDPR, and if you set the requirements right, this same infrastructure can underpin your business' future for driving greater revenue.

By applying this initiative to fund a proper centralized transparent AI underpinned by solid data, integration, and automation capabilities, you can use the moment to accelerate past your competition with new "super-powers" that create greater relevance, revenue, and retention. That is, if you work with the right partner.

Powering your GDPR strategy with Pega

To help establish your system – to manage the systems – to handle GDPR, you need powerful capabilities for orchestration, governance, dynamic processes, and auditability. And this feat of digital process automation must span across your entire enterprise.

This involves digitizing current manual processes, and automating dynamic, complex processes, even across systems that may not have accessible APIs. And if you think you can solve the problem by writing more brittle "spaghetti code" – think again. Not only is writing code a dated approach, it will never provide the speed and scale needed to comply, and stay compliant, with GDPR.

As the world leader in digital process automation, according to Gartner, Pega is uniquely equipped to empower your business to take on GDPR, with intelligent and adaptive technology.

f in 🐦

PEGA®

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**