Everest Group® RESEARCH

GDPR Compliance – Can Automation Save the Day?

Sarah Burnett, Vice President
Anil Vijayan, Practice Director
Nukul Upadhye, Senior Analyst

UiPath

Summary

With GDPR in effect as of May 25, 2018, many organizations are grappling with the massive changes that the regulation mandates from the technology, process, and people perspectives. Robotic Process Automation (RPA) has a significant role to play in alleviating some of this pain. In this paper, we examine and discuss:

- GDPR and its implications for organizations, particularly in terms of administrative overheads
- The role that RPA can play in helping automate GDPR-related administrative tasks and functions
- The implications of GDPR on sourcing / service delivery models and the RPA angle in such decisions
- The case for digital transformation and superior analytics driven by GDPR compliance, and a framework to work through the automation play

EGR-2018-X-V-XXXX

Introduction

"However fast regulation moves, technology moves faster. Especially as far as data is concerned."

Elizabeth Denham, UK Information Commissioner

In April 2016, the European Parliament adopted the European Union General Data Protection Regulation (GDPR) – officially EU 2016/679 – which came into effect May 25, 2018. GDPR replaces the existing data privacy regulation, the 1995 EU Data Protection Directive (DPD), and introduces new, stricter provisions, particularly around personal data. The legislation directly impacts all companies based in, or doing business with, companies/ individuals based in the European Economic Area (EEA), which comprises the EU, Norway, Iceland, and Liechtenstein.

GDPR defines personal data as data by which an individual becomes identified or identifiable, whether directly or indirectly, by all means reasonably likely to be used.

The definition, which previously included only names, physical, physiological, social, mental, economic, cultural, and mental identifiers, has been extended to include locations data, online identifiers, racial origin, religious beliefs, political opinions, trade union membership, health life, sex life, genetic identifiers, and biometric identifiers. This signifies that the "personal data" would include all identification-enabling information, from names, IP addresses, internet cookies, and mobile device IDs to fingerprints and retinal data.

A gray zone exists for multiple types of data, as chances of identifying an individual depend on the presence of other associated data with the data controller. For example, a name may not qualify as personal data in itself; however, if a controller possesses the place of work data for the same individual, it then becomes personal data.

Several issues drive the need for this new data protection regulation:

- Rapid advances in technology since the 1995 regulation was framed
- Increasing number of data breaches
- Increasingly aggressive business practices, often involving misuse/abuse of personal data
- Little actual control of individual citizens over the use of their personal data

With serious financial and reputational risks associated with GDPR non-compliance, it is imperative that all organizations take action to ensure compliance; and those that are behind in adoption are especially at risk. This is where Robotic Process Automation (RPA) can play a critical role. Through the use of RPA, organizations can address large portions of GDPR compliance relatively quickly and cost effectively. While not a panacea, RPA promises to help set non-compliant organizations on the right track almost immediately.

EGR-2018-X-V-XXXX

Implications of GDPR on enterprises and the role of RPA

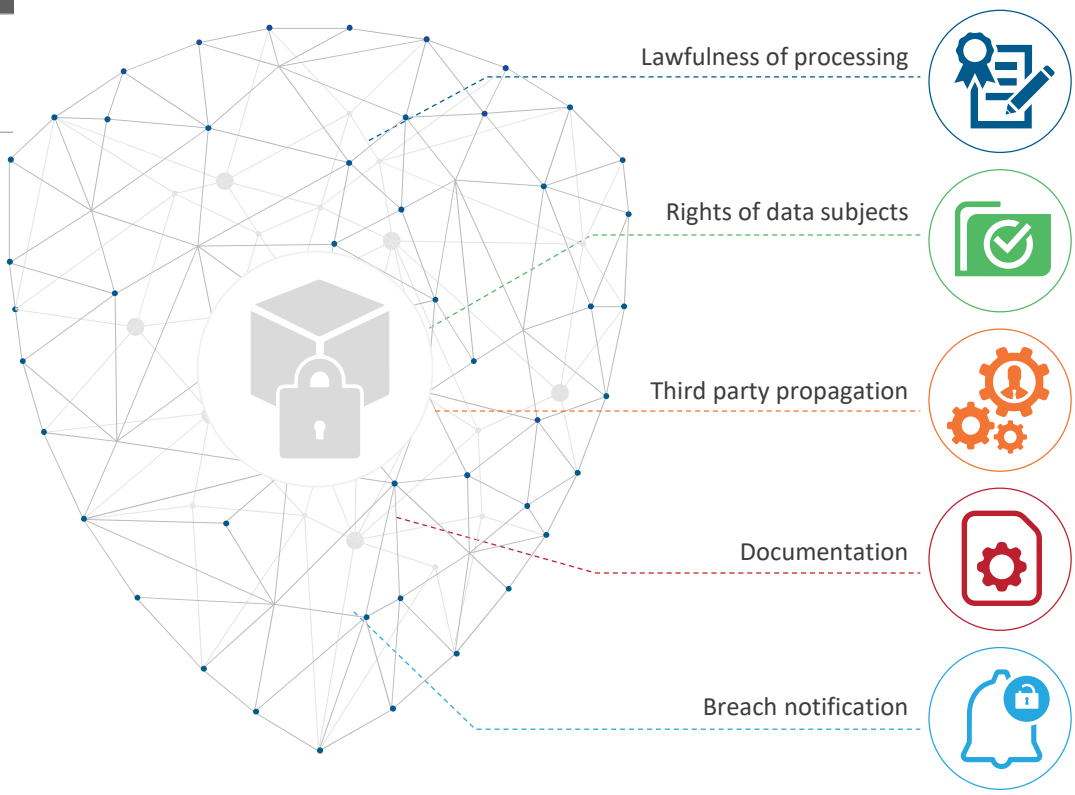
Direct impact – administration

Organizations must make significant changes to the way they handle data to comply with GDPR. These changes drive up the cost of administrative overheads. RPA, with its ability to manage repetitive, rules-based tasks, can help reduce administrative costs and avoid processing errors. Exhibit 1 illustrates a few of the key areas in which RPA is applicable.

EXHIBIT 1

Implication of GDPR on administrative overheads of enterprises

Source: Everest Group (2018)



Lawfulness of processing

All data processing must a valid business reason (as laid out in Article 6 of GDPR) , such as the need to fulfill a contract or the performance of a task carried out in public interest. The biggest challenge to ensuring compliance is the complexity in mapping data to know what data is stored where within the organization. For existing structured data, software robots can identify and classify personal information that is stored on an organization's system. For unstructured data, identifying personal information would require more sophisticated techniques including natural language processing and/or machine learning capabilities beyond traditional RPA. Once consent has been determined or captured, robots can be used in conjunction with consent management databases/systems to action (typically delete) data based on consent rules such as holding period.

EGR-2018-X-V-XXXX

Rights of data subjects:

Pursuant to GDPR, organizations must implement mechanisms to fulfill certain rights, such as the right to be forgotten (or, more accurately, to data erasure), the right to rectification, the right to data portability, and the right to access.

GDPR makes consent management an ongoing activity. Companies must be able to show data subjects all of the information the company has related to them upon request. They must also be able to update or delete their personal information or revoke the consent to use it for specific purposes.

In the absence of RPA, complying with this mandate can be highly manual and error prone; RPA can both automate processes and reduce errors. For instance, enterprises set up a portal where individuals can file GDPR-related requests. Through this portal they can update/delete their personal information or request access to personal information stored. Every time a data subject enters his/her details on the portal, robots would search all client systems and present a unified view of all instances of personal data use for that individual.

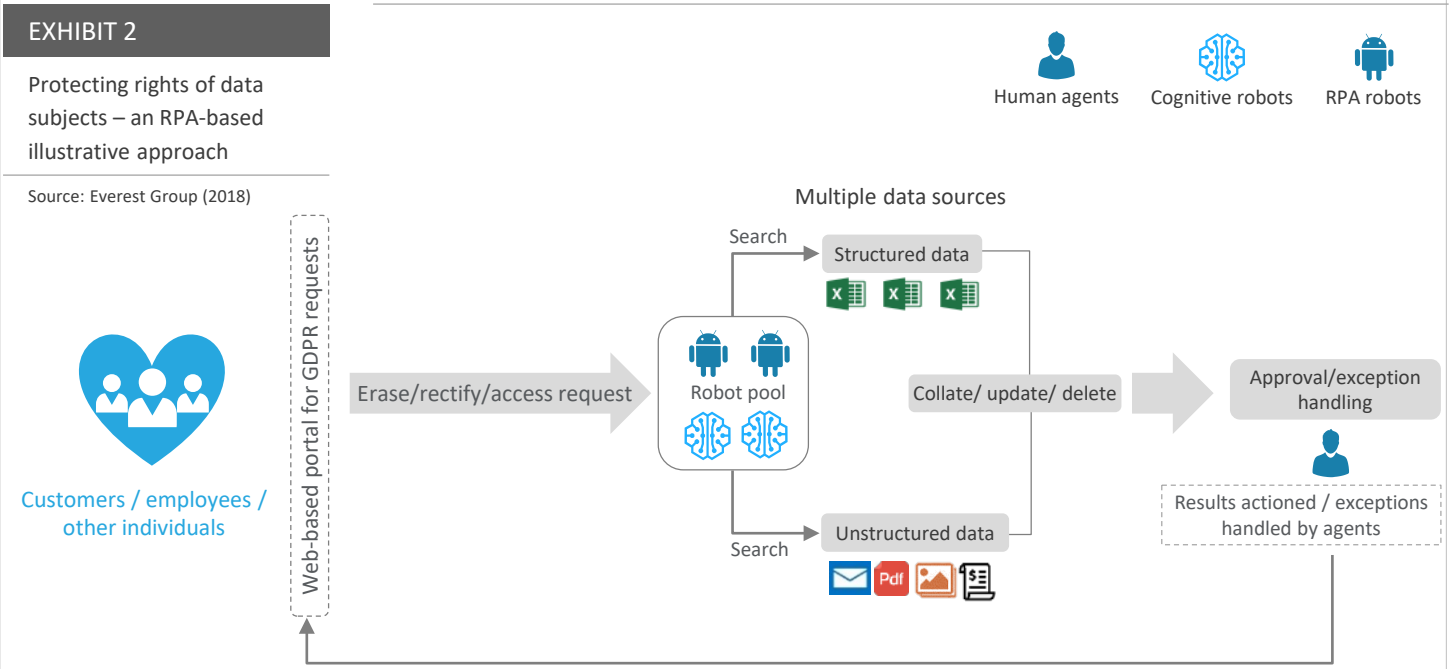
The user can see what information is stored. Similarly, when the user wants to update personal information, robots would help propagate changes to all that individual's records throughout the organization's systems, ensuring that the individual can easily exercise his/her right to rectification and/or the right to be forgotten. Thus RPA can help organizations to:

- Promptly respond to individuals' requests
- Cost effectively manage large volumes of data access/update/deletion requests
- Maintain an audit trail of all requests

EXHIBIT 2

Protecting rights of data subjects – an RPA-based illustrative approach

Source: Everest Group (2018)



EGR-2018-X-V-XXXX

Third-party propagation:

For an enterprise to be compliant with GDPR, its vendors and suppliers – including outsourcing partners – must also be compliant as data processors, since data subject rights extend to these third parties as well. For instance, in the case of a request to be forgotten, the data controller (the enterprise) must ensure that the data processor the (third party vendor) erase relevant data as well. Robots can help either by using the vendor's portal to log the propagated request with specific details or by using other communication channels, such as email, to pass on the request.

Additionally, vendors that use RPA to comply with GDPR are in a better position to help enterprises to comply with GDPR-related requests and hence may be favored going forward.

Documentation:

Organizations must maintain records of data-processing activities and be ready to present them to regulators upon request. To effectively comply, an organization must know and record how personal data is processed by all departments and employees within the organization.

Because software robots generate activity log files containing every action they take, any data addition, update, or deletion is recorded. As organizations make greater use of RPA to manage most of their transactional data processing, activity logs become richer and more comprehensive, increasing their utility as audit documentation. Ultimately, automating tasks such as consent management and management of personal information serves a dual purposes: it increases efficiency and accuracy, and also aids in audit preparedness.

Breach notification:

Data breaches likely to result in high risk to individuals' rights and freedoms must be reported to the authorities within 72 hours, and subsequently to the data subjects as well, in certain cases.

Given the frequency of data breaches in the recent past, organizations must take every step to avoid data breaches and inform data subjects in case of a breach. In this regard, RPA can help enterprises in two ways:

- Avoiding data breach: Robots can be used to execute the process of de-identifying data before storing it in the organization's systems. De-identifying data can help avoid the release of personal information in the event of a breach
- Breach notification: In the event that personal information is leaked, enterprises can use RPA to notify all data subjects within the compliance window

While RPA can help with data security issues, enterprises must be careful not to open up new avenues for potential data breaches through poor security practices during implementation and operationalization. They must ensure that the chosen RPA vendor has all the necessary provisions in place, including encryption of passwords, robust user access control mechanisms, etc. Some enterprises might also require that the robots are run behind locked screens or through headless virtual terminals. Security checks on any operator that can see the robots in operation may be necessary as well.

EGR-2018-X-V-XXXX

EXHIBIT 4A

RPA utility and use cases for GDPR stipulations

Source: Everest Group (2018)

○ Low ● High

GDPR stipulation	RPA utility for compliance	Use cases
Lawfulness of processing		• Finding, matching, authenticating, and mapping personal information in structured data • Actioning data per consent management guidelines • Updating individuals' consent status, records/logs and maintaining an audit trail
Rights of data subjects		Fulfilling right to access, right to be forgotten, right to rectification, etc. for structured data
Third-party propagation		Extension of fulfillment of requests around right to access, erasure, etc.
Documentation		Creating audit trails to track data usage
Breach notification		Notification of breach to data subjects using pre-defined templates for automated letters / emails / text messages

Indirect impact – services delivery model

As a consequence of GDPR, organizations will likely scrutinize outsourcing decisions and sourcing constructs more closely. GDPR directs that controllers choose processors that are GDPR compliant or risk penalties themselves. Additionally, GDPR necessitates that data be managed in EEA jurisdictions or jurisdictions that are deemed to be equivalent to it. While there is no direct mandate on suitable locations in the regulation itself, locations that have a good data protection track record as well as accessible legal systems that offer enforceability/compatibility with GDPR are naturally preferable. Sourcing of back office functions are likely to be affected in two ways:

Insourcing vs outsourcing

Some enterprises may want to reconsider outsourcing for critical processes, particularly those that deal with high risk data such as credit card information. A breach impacting this type of data generally attracts higher scrutiny, so organizations may want to bring them in-house where they can exercise a higher degree of control.

Additionally, they may prefer EEA regions for delivery of such processes, which could mean a movement of data from cloud-based providers to in-house data centers, as well as a movement of outsourced processes back in-house. RPA can play a significant role in alleviating some of the cost concerns around such a move, particularly if the process in question is rules-based and transactional (as tends to be the case in a major portion of outsourcing constructs). Through diligent application of RPA, an enterprise, can bring down the cost differential between an outsourcing provider (which uses economies of scale and offshoring levers to reduce cost) and an in-house version, even one located in a high cost EEA region.

EGR-2018-X-V-XXXX

Service provider selection

Outsourcing service providers typically fall under the processor category when viewed from an enterprise perspective. Enterprises must ensure that their processors are GDPR compliant. There is a varying degree of readiness among service providers. A conservative approach would be to re-examine contracts with providers that may be high risk and migrate concerning contracts to an existing low-risk service provider.

It is essential to note that good data management practices are vital for full compliance with both the letter and the spirit of the GDPR regulation; without them, RPA is ineffective. However, with good practices as a baseline, RPA can play a significant role in implementing GDPR measures efficiently, accurately, and cost effectively.

Going beyond compliance

Opportunity for well-structured digital transformation

GDPR mandates privacy by design. As a result, full compliance would likely require a re-examination of the technology, people, and process landscape within the organization. Given that non-compliance has massive financial and reputational risks, most organizations, particularly EU-centric ones, will need to embark on this transformative journey if they have not done so already. This exercise will likely be organization-wide, touching almost all aspects of the organizational landscape and hence is naturally a good opportunity for organizations to implement digital transformation as well.

Many organizations today operate with fragmented systems and poorly designed processes. A digital transformation would set out to refocus processes on customer centricity, replace and/or build bridges among disparate systems and departments, and introduce more efficiency in processes by reducing human intervention in transactional, rules-based tasks. RPA can help with each of these goals, particularly automation of transactional tasks, and is often a part of digital transformation initiatives today.

However, in applying RPA within the digital transformation journey, organizations should ideally:

- Identify a long list of potential process areas for application of automation
- Prioritize subprocesses within those processes using metrics that emphasize both ROI and compliance (with GDPR amongst other regulations)
- Identify use cases and run quick-win pilots before proceeding with a large scale, preferably phased, organization-wide roll out

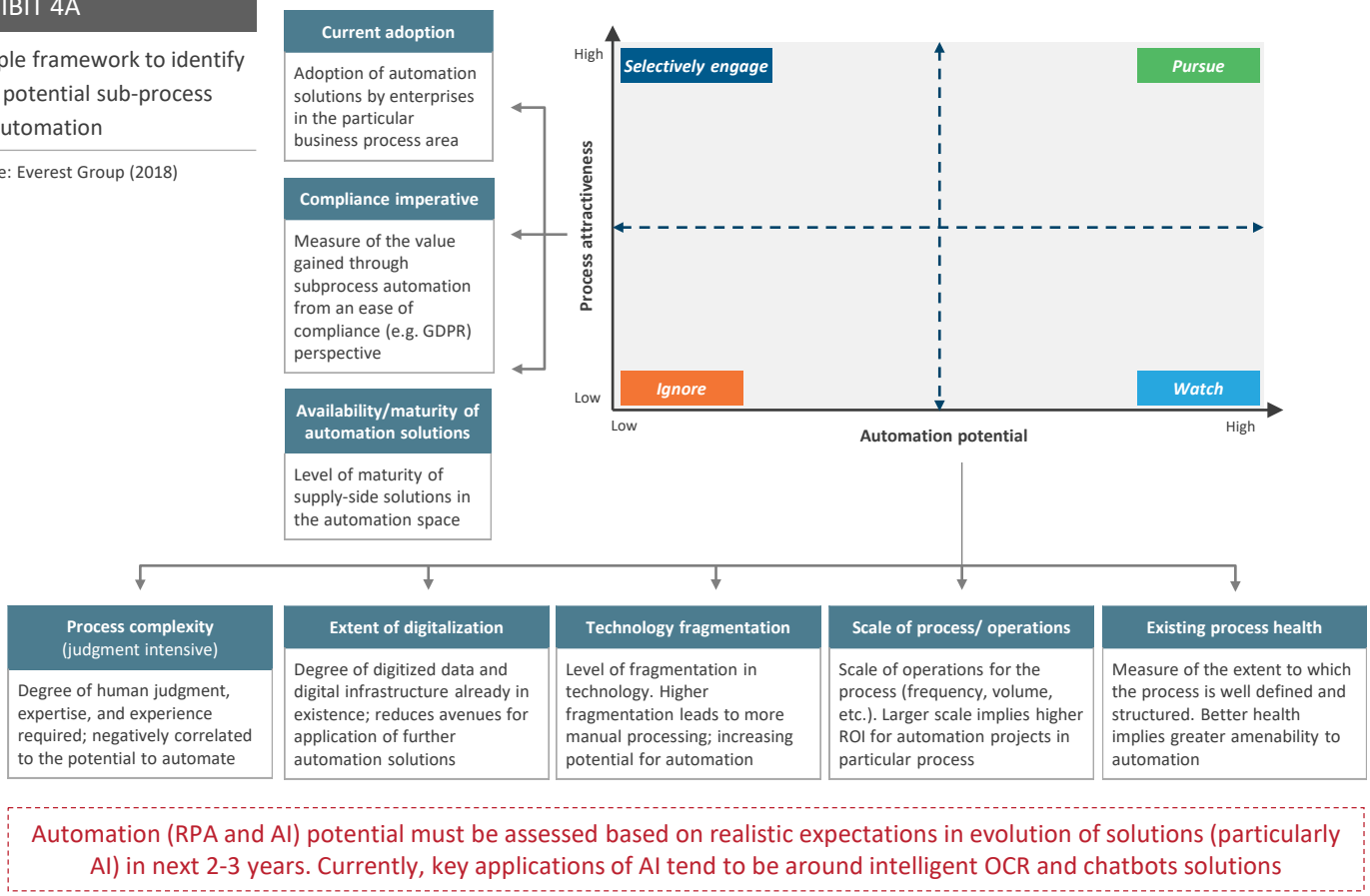
The use of a framework such as the one in Exhibit 4 can help achieve this outcome in a structured fashion. Exhibit 4a provides the overview of the framework. Exhibit 4b provides an example for HR processes.

EGR-2018-X-V-XXXX

EXHIBIT 4A

Sample framework to identify high potential sub-process for automation

Source: Everest Group (2018)

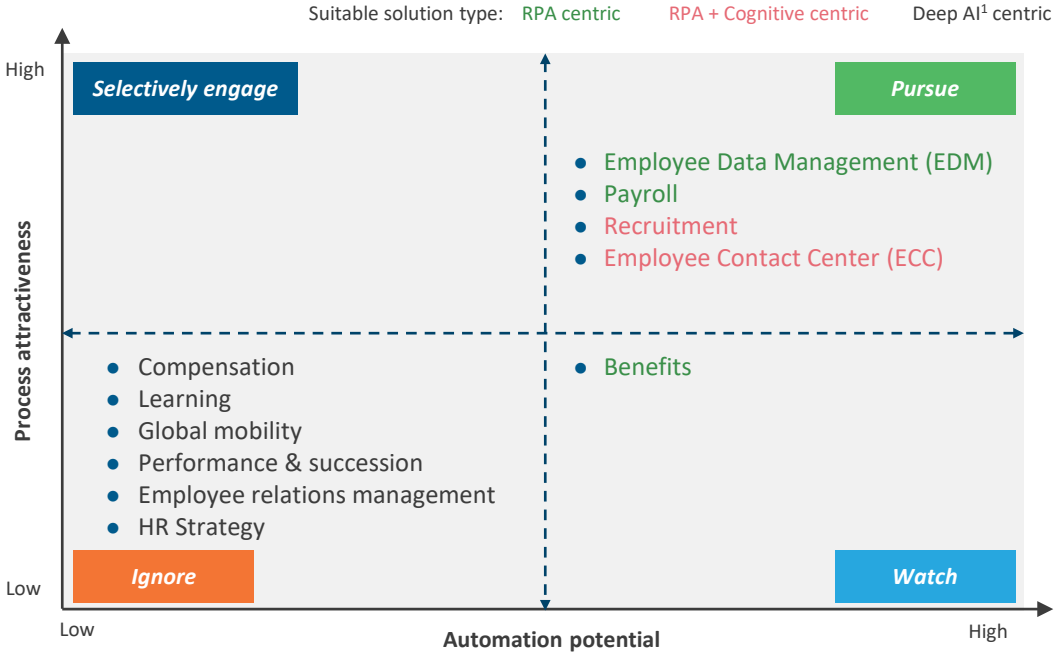


Automation (RPA and AI) potential must be assessed based on realistic expectations in evolution of solutions (particularly AI) in next 2-3 years. Currently, key applications of AI tend to be around intelligent OCR and chatbots solutions

EXHIBIT 4B

Example: Applying the framework for HR (see Appendix for details) and identifying high potential sub-processes

Source: Everest Group (2018)



1 Refers to solutions with very deep AI and high level of sophistication; unlikely to have any meaningful adoption based on the current maturity

EGR-2018-X-V-XXXX

Such a structured approach would not only ensure that investments flow to the right areas, but also help leaders to think through the art of the possible when it comes to relatively new and/or unexplored process areas for the application of automation.

GDPR thus presents an opportunity for broad-based application of RPA within enterprises.

Breaking data silos for customer delight

As a result of GDPR, organizations will have to map their sources and locations of personal data throughout the organization, which provides the opportunity to create a consolidated view into customer and prospect data stored across otherwise seemingly impenetrable barriers. Similar to a right to access portal, RPA can enable internal (to enterprise) access and consolidation of data, for a particular customer, for example. This data would otherwise be siloed and difficult to access internally. A consolidated view of this data could be a gold mine for application of analytics, seeking to better the experience of customers and prospects alike. Enterprises can use this data in multiple ways (assuming permission in all cases):

- Provide targeted upsell and cross sell information to relevant customers
- Understand various customer pain points and implement initiatives to rectify them
- Introduce any of a host of customer behavior / needs predictive analytics applications

While the key driver for organizations would be compliance with GDPR, the opportunity to derive better customer insights and digitally transform the organization is a significant added benefit.

EGR-2018-X-V-XXXX

Conclusion

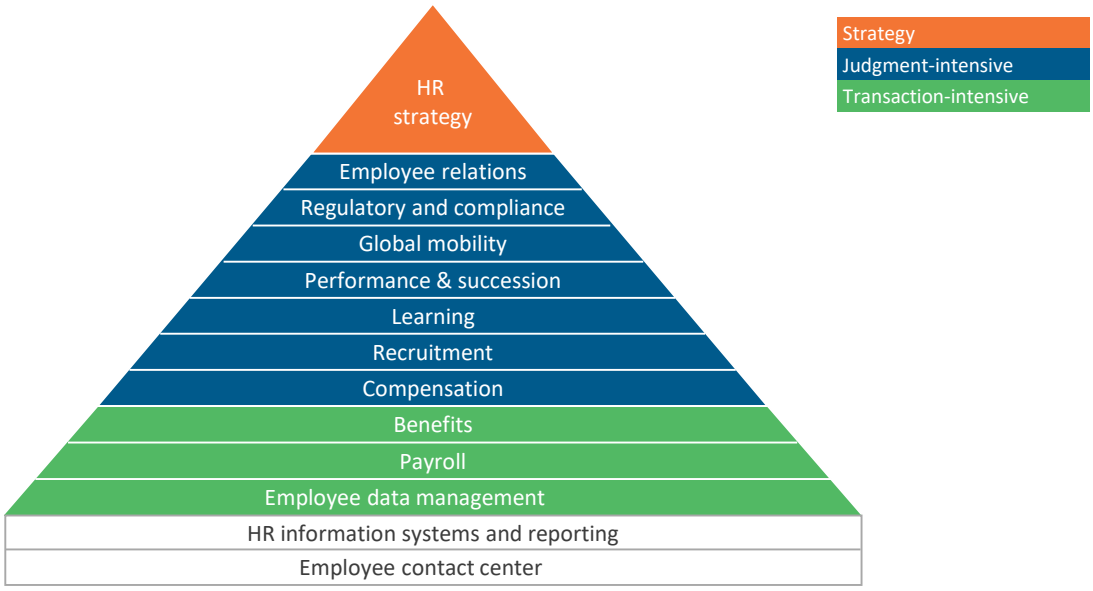
GDPR is one of the most stringent and comprehensive data regulations in the world today. With fines of up to 20 million euros or 4% of annual turnover (whichever is higher), the financial risk to organizations is immense. Add to that the reputation risks, and one can easily anticipate a situation in which even large organizations could be put out of business in the event of non-compliance.

While the regulation came into effect on May 25th 2018, several organizations are yet to take concrete steps to ensure full compliance. There are multiple issues that organizations grapple with in implementing the necessary measures, including lack of understanding, substantial cost, and time to implement. Robots, with their ability to work non-intrusively and efficiently, could be an ideal solution for organizations looking for opportunities to comply with GDPR quickly. While automation may not provide a complete solution, it can certainly ensure compliance with large parts of the regulation quickly and cost effectively.

For organizations looking for a much more systematic approach, RPA still plays a role, perhaps an even larger role. As they look to redesign their process and technology landscapes, they should keep in mind the opportunity to transform operations using RPA and other digital levers. In combination with technologies such as analytics, organizations can even use this compliance mandate to transform and gain a competitive advantage in the market.

EGR-2018-X-V-XXXX

Appendix – HR business process value chain



Strategy

- Policies
- Procedures
- HR job profiles
- Budgeting/forecasting
- Workforce planning
- M&As/divestitures
- Values and ethics
- HR strategy development

Employee relations

- Strategy
- Performance / conflict resolution
- Union relations
- Employee assistance programs
- Communication
- Vendor management

Regulatory & compliance

- Strategy
- Workforce diversity and anti-discrimination
- Government reporting
- Claims/audits
- Visas
- Exit administration
- Vendor management

Global mobility

- Strategy and policy development
- Assignment package
- Pre-departure activities
- On-assignment activities
- Property services
- Moving services
- Policy exceptions
- Tax planning administration
- Vendor management

Performance & succession

- Strategy
- Career development
- Succession planning
- Performance surveys
- Collation and analysis
- Disciplinary actions
- Vendor management

Learning

- Strategy
- Curriculum development
- Content design
- Content development
- Content management
- Registration management
- Scheduling
- Evaluation management
- Vendor management

Recruitment

- Strategy
- Sourcing
- Screening
- Applicant tracking
- Interview scheduling
- Assessment
- Background checking
- Offer letter management
- Onboarding
- Vendor management

Compensation

- Strategy
- Job analysis/descriptions
- Job pricing
- Base pay adjustments
- Salary administration
- Bonuses/incentives/awards
- Stock options/purchase program
- Commissions/draws
- Compensation statement
- Vendor management

Benefits

- Strategy
- Healthcare plans
- Defined benefit plans
- Defined contribution plans
- Workers' compensation
- Leave programs (e.g., LOA)
- Health and safety
- Vendor management

Payroll

- Strategy
- Payroll preparation (build to gross)
- Payroll calculation (gross to net)
- Payroll distribution
- Reconciliation
- Third-party payments
- Payroll tax reporting and filing
- Vendor management

Employee data management

- Employee data changes
- Status changes
- New hire processing
- Transfer processing
- Timekeeping
- Cost center assignments
- Time and expense administration
- Unemployment administration
- Exit administration
- Vendor management

EGR-2018-X-V-XXXX

About Everest Group

Everest Group is a consulting and research firm focused on strategic IT, business services, and sourcing. We are trusted advisors to senior executives of leading enterprises, providers, and investors. Our firm helps clients improve operational and financial performance through a hands-on process that supports them in making well-informed decisions that deliver high-impact results and achieve sustained value. Our insight and guidance empower clients to improve organizational efficiency, effectiveness, agility, and responsiveness. What sets Everest Group apart is the integration of deep sourcing knowledge, problem-solving skills and original research. Details and in-depth content are available at www.everestgrp.com.

This study was funded, in part, by UiPath

For more information about Everest Group, please contact:

+1-214-451-3000
info@everestgrp.com

For more information about this topic please contact the author(s):

Sarah Burnett, Vice President
sarah.burnett@everestgrp.com

Anil Vijayan, Practice Director
anil.vijayan@everestgrp.com

Nukul Upadhye, Senior Analyst
n.upadhye@everestgrp.com