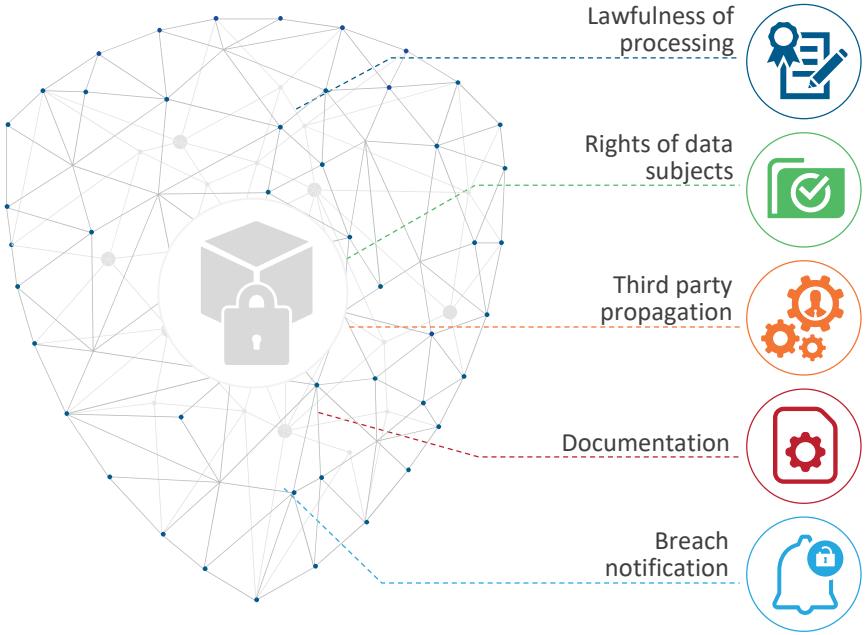
GDPR is one of the most stringent

and comprehensive data regulations in the world today. With fines for noncompliance 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 if they do not comply.

Obviously, organizations must make significant changes to the way they handle data to comply with GDPR. However, these changes could significantly increase the cost of administrative overheads. Everest Group research shows that RPA, with its ability to manage repetitive, rules-based tasks, can help reduce administrative costs and avoid processing errors. Figure 1 illustrates a few of the key areas in which RPA is applicable.

Figure 1 *Implications of GDPR on enterprises' administrative overheads*



Implications of GDPR on enterprises' administrative overheads

Lawfulness of processing

All data processing must have a valid business reason, such as the need to fulfill a contract or the performance of a task carried out in the public interest. The biggest challenge to ensuring compliance is the complexity in mapping data to know what data is stored where within the organization.

Rights of data subjects

GDPR requires organizations to 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.

The regulation makes consent management an ongoing activity: companies must be able to show data subjects all company-held information that is related to them upon request. They must also be able to update or delete a subject's 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 can set up a portal where individuals can file GDPR-related requests. 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

Figure 2 illustrates an RPA-based approach to protecting data subjects' rights.

Third-party propagation

For an enterprise to comply with GDPR, its vendors and suppliers – including outsourcing partners – must also be compliant as data processors, because data subject rights extend to these third parties 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.

Documentation

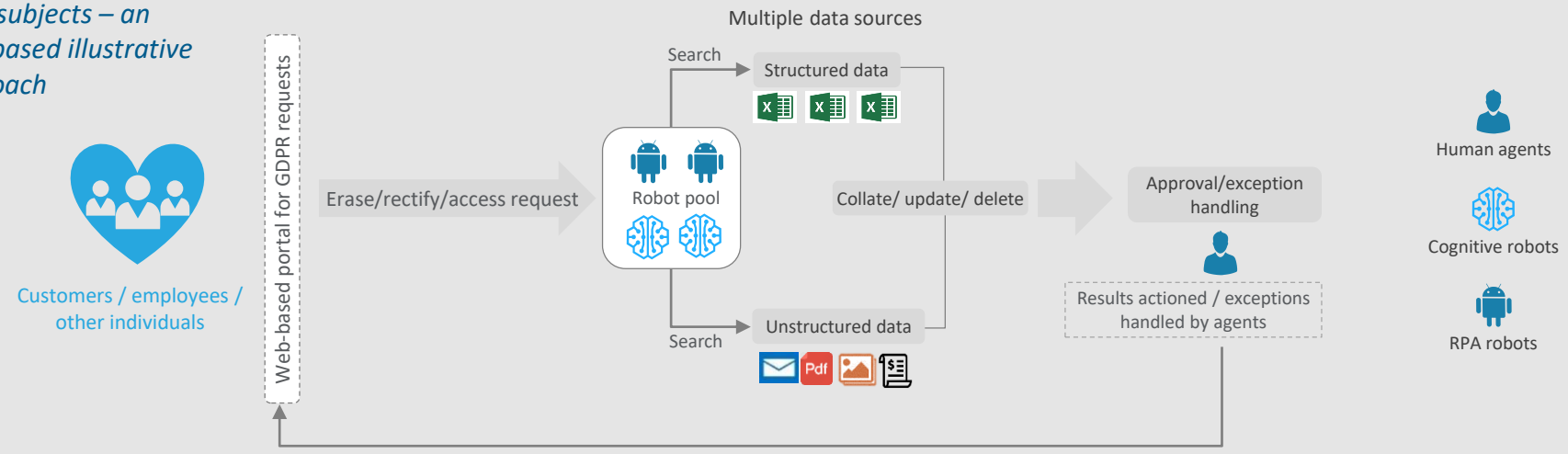
Organizations must maintain records of data processing activities and be ready to present them to regulators upon request. To effectively comply, an organization must know and record how personal data is processed by all departments and employees within the organization.

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.

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.

Figure 2 *Protecting rights of data subjects – an RPA-based illustrative approach*



Given the frequency of data breaches in the recent past, organizations must take every step to avoid them 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 timeframe

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.

Indirect impact – services delivery model

As a consequence of GDPR, organizations are likely to scrutinize outsourcing decisions and sourcing constructs more closely. GDPR directs controllers to select processors that are GDPR compliant or risk penalties themselves. Additionally, GDPR requires that data be managed in European Economic Area (EEA) jurisdictions or jurisdictions deemed to be equivalent. As a result, sourcing of back office functions is likely to be affected in two ways:

Insourcing vs. outsourcing

Enterprises may reconsider outsourcing of critical processes, particularly those that deal with high-risk data, such as credit card information, as breaches impacting this type of data generally attract higher scrutiny. In addition, enterprises may prefer EEA regions for delivery of these processes, which could mean moving data from cloud-based providers to in-house data centers, or outsourced processes back in-house. In these cases, RPA can play a significant role in cost reduction, particularly for rules-based and transactional processes, which tend to be the majority in these constructs.

Service provider selection

Outsourcing service providers are typically considered processors; under GDPR, enterprises must ensure that their processors are GDPR compliant. Enterprises should re-examine contracts with providers that may be high risk and migrate concerning contracts to an existing low-risk service provider.

+++ +++ +++

As a final point, 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.

For more information on this topic, including how GDPR + RPA can benefit your organization beyond compliance, see our full report, *GDPR Compliance – Can Automation Save the Day?*

Additional Resources

- EU GDPR: What Does the Disruption Mean for Your Industry
- GDPR Services: Gross Disconnect in Perception and Reality - Services PEAK Matrix™ Assessment 2018
- Robotic Process Automation (RPA) Annual Report 2018 – Creating Business Value in a Digital-First World
- Defining Enterprise RPA

About Everest Group's Market Insights™

Everest Group's Market Insights reveal actionable intelligence from across the full spectrum of our research in concise, easily accessible infographics

To view more Market Insights visit www.everestgrp.com

Dallas (Headquarters)
info@everestgrp.com
+1-214-451-3000

Bangalore
india@everestgrp.com
+91-804-276-4533

Delhi
india@everestgrp.com
+91-124-496-1000

London
unitedkingdom@everestgrp.com
+44-207-129-1318

New York
info@everestgrp.com
+1-646-805-4000

Toronto
canada@everestgrp.com
+1-416-388-6765

Stay connected

Website

www.everestgrp.com

Social Media

@EverestGroup

@Everest Group

Blog

Sherpas In Blue Shirts

www.sherpasinblueshirts.com