



EU GDPR: Is There a Silver Lining to the Disruption?

An Evaluation of the Impact of
the European Union General Data
Protection Regulation (GDPR) on
Global Services Delivery

Eric Simonson, Managing Partner
Julian Herbert, Vice President
Anurag Srivastava, Vice President
Chirag Bhatia, Senior Analyst

Copyright © 2017, Everest Global, Inc. All rights reserved.

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 will come into effect in May 2018. The regulation, referred commonly to as GDPR, replaces the existing data privacy regulation, the 1995 EU Data Protection Directive (DPD), and introduces new, stricter provisions. 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 a living 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 & retinal data.

A grey zone exists for multiple types of data, as chances of identifying a living person depend on the presence of other associated data with the data controller. For example, “name” may not qualify as personal data in itself; however, a controller possessing the “place of work” data for the same individual becomes personal data.

Key drivers for a new data protection regulation include:

- Rapid advances in technology since the 1995 regulation was framed
- Increasing instances 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

The proposed regulation is significantly more stringent compared to the existing directive; key changes are highlighted in Exhibit 1:

EXHIBIT 1

Key changes proposed by
GDPR

Source: Everest Group (2017)



For a more detailed summary of key changes and new provisions, please refer to the Appendix section on pages 8 and 9.

This viewpoint aims to look beyond the short-term impact (tactical changes to achieve compliance) at the long-term and far-reaching strategic impact on global services delivery.

Impact on global services delivery

Owing to the stringent and punitive provisions of GDPR (especially the possibility of multi-million euro fines for non-compliance), we believe that all organizations that hold or process personal data will experience some disruption in service delivery. This will span not just delivery portfolios based in the EEA, but global delivery portfolios across functions (IT, business process, contact center, and digital services).

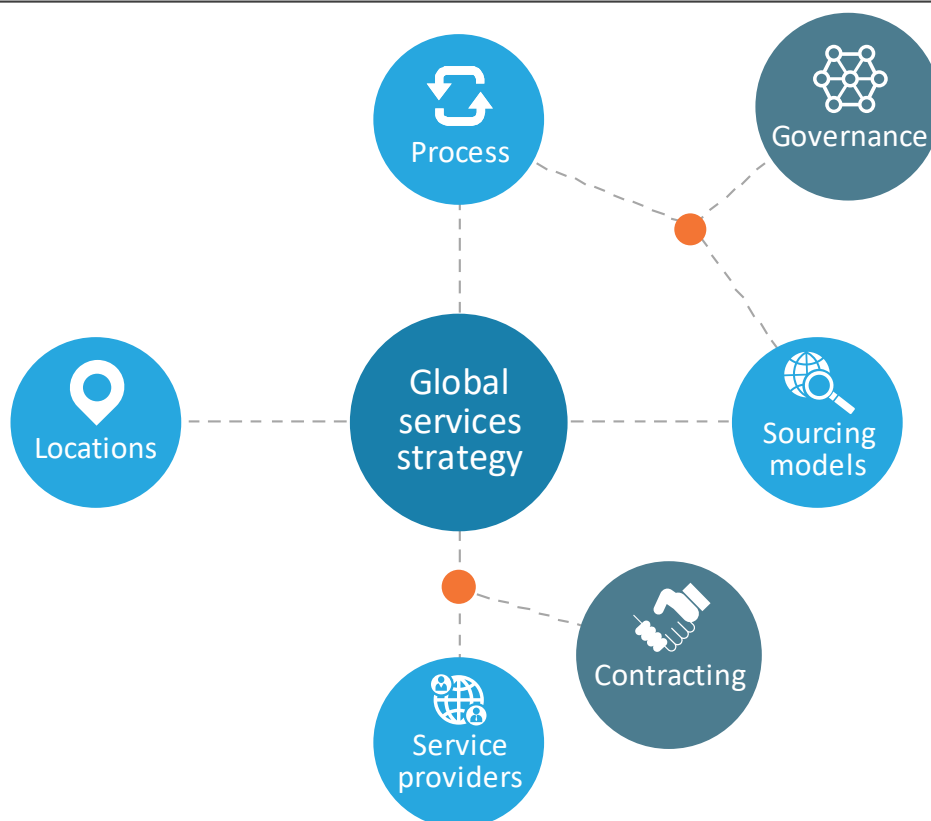
We evaluated the impact of GDPR on the key components of global services delivery strategies, as explained in Exhibit 2 below.

EXHIBIT 2

Key components of global services delivery strategy

Source: Everest Group (2017)

“The GDPR must be hailed as an awesome step in the direction of promoting the rights of natural persons and should ultimately strengthen global relations and commerce.”
– Schellman & Company



We expect GDPR to result in the following types of disruption in global services delivery in an organization:

Increased overheads: Compliance with the provisions of GDPR will add layers of additional steps, checks/oversight, and documentation to service delivery and other governance-related processes

Opportunity for transformation: GDPR is also likely to provide a push or an added incentive for transformation of service delivery elements, e.g., process redesign, increased leverage of technology, and delivery model transformation

Push towards consolidation: GDPR will also lead to significant consolidation in multiple delivery model elements (e.g., locations and providers) as enterprises/collectors try to reduce their exposure to potential avenues of breach in compliance

The next few pages evaluate the extent of impact across the components of service delivery and describe what the respective impacts will be.



Process

Extent of impact from GDPR

- Increased overheads
- Opportunity for transformation
- Push towards consolidation

Comprehensive mapping of data flows for existing and new processes

- Data Privacy Impact Assessments (DPIA) to identify high risk processes
- Data flow mapping across processes to:
 - Ensure compliance with new consent and notification obligations, as well as new data subject rights
 - Ensure that potential leakage avenues are identified, tracked, and possibly plugged
 - Categorize personal data by the parameters of sensitivity, legal justification for holding it, and duration of holding data

Redesign and transformation of processes

- Significant investments into structural transformation of processes for “privacy by design” and reduction of risk exposure to ensure:
 - Compliance with all new data rights, including erasure and portability
 - Anonymization of data, wherever reasonably possible
 - Reduction in data breach exposure (for high risk processes, organizations must engage with an appropriate data protection authority before processing can take place, thereby leading to significant potential impact on delivery timelines. Transformation of such processes will be imperative)
- Organizations will leverage technology (including automation and digitalization) to:
 - Ensure compliance with new data security policies
 - Reduce human access to data
 - Transform processes to plug leakage/breach avenues



Sourcing models

Extent of impact from GDPR

- Increased overheads
- Opportunity for transformation
- Push towards consolidation

Rebalancing across sourcing models

- Rebalancing of processes across sourcing models (in-house / outsourced / hybrid), depending on risk appetite:
 - In-sourcing of processes that present high breach risk, to ensure better control
 - Possible fillip to hybrid models that can offer advantages of both in-house (stronger control mechanisms) and outsourcing models (access to specialist expertise)



Service Providers

Extent of impact from GDPR

- Increased overheads
- Opportunity for transformation
- Push towards consolidation

Consolidation of service provider portfolio

- Significant due-diligence on service providers, followed by consolidation of providers in the portfolio; winners (or survivors, whichever you deem has the correct emphasis?) will show leadership in adapting to change and willingness to be enterprises' partners in this transformation.
- Skepticism towards cloud service providers owing to lack of certainty/transparency around location of data
- Possible preference towards EEA-based service providers as these may be perceived to be more reliable (by virtue of operating inside EU jurisdiction) and easier to deal with, in case of non-compliance

Upheaval in service provider landscape

- Mergers and acquisitions:
 - Smaller providers may lack resources to invest in ensuring compliance, while large providers may have resources, but may lack the agility to achieve compliance quickly enough to retain clients
 - Providers that are unable to demonstrate the ability to adapt quickly may get left behind and seek exits
- Emergence of a new breed of providers that demonstrate leadership in achieving compliance and adapting to change through leverage of innovative models and technology



Locations

Extent of impact from GDPR

- Increased overheads
- Opportunity for transformation
- Push towards consolidation

GDPR implies that data is managed in EEA jurisdictions or jurisdictions that are deemed to be equivalent to it. This directly impacts where personal data can and cannot be handled, thereby determining where different parts of the delivery model are located. This will lead to the following results:

Consolidation of locations portfolio

- While there is no direct mandate on suitable locations in the regulation itself, organizations will consolidate to locations that offer an attractive data protection track record as well as accessible legal systems that offer enforceability/compatibility with GDPR

Preference for EEA locations, especially for high-risk processes

- Enterprises and service providers may ramp up delivery presence in the EEA, especially for high-risk processes

Apart from ensuring adequate compliance, the above shifts to lower-risk locations also offer controllers protection in case they are sued for mistakes made by processors and they want to counter-sue these processors.



Governance

Extent of impact from GDPR

- ☒ Increased overheads
- ☒ Opportunity for transformation
- ☐ Push towards consolidation

Heightened importance of specialist Data Protection Officers

- Whilst the appointment of a Data Protection Officer (DPO) is not mandatory for all companies, the requirement to demonstrate compliance with GDPR means that the appointment of a specialist DPO will be commonplace. It will become a “hygiene factor”, especially for service providers
- The DPO will be involved heavily in governance of in-house or outsourced delivery, as organizations must be able to demonstrate that all matters relating to the processing of personal data are compliant with GDPR

Focus on data protection

- Governance best practices will include data protection; organizations will employ compliance mechanisms including revised data protection policies, codes of conduct, and additional training to ensure compliance where human access is involved
- The highest levels of management will have a direct interest in ensuring compliance and, by necessity, will need to be involved in ensuring compliance



Contracting

Extent of impact from GDPR

- ☒ Increased overheads
- ☒ Opportunity for transformation
- ☐ Push towards consolidation

Redesign of contracts



















- The respective allocation of duties/responsibilities with regard to data protection between client organizations and service providers will need to be explicitly stated in contracts
- Whilst liability of data controllers and processors in the event of a breach caused by negligence of both parties can be contractually allocated, it will legally be “joint and several”
- Downstream processors will have to agree to all GDPR requirements
 - Controllers might require non-EU processors to have offices in EU for accountability
 - Controllers might require processors to get data protection-related certifications from standards’ bodies such as ISACA, CREST, or BCS (see Appendix).

Renegotiation

- Significant renegotiation of contracts expected owing to:
 - High initial cost incurred by processors for ensuring compliance
 - Increase in cost of delivery even in steady state from overheads related to reporting readiness and subject rights, and from continuous updates to security procedures arising from evolving regulations

Conclusion

The table below summarizes the extent of disruption across the key components of global delivery strategy:

Components of global delivery strategy	Types of disruption			Comments
	Increased overheads	Opportunity for transformation	Push towards consolidation	
Process				Overall, GDPR poses the risk of significant disruption to global service delivery. While some components (processes, governance, and contracting) will present substantially increased overheads largely on account of additional documentation and oversight; parameters such as sourcing models, service providers, locations, and (to some extent) process, offer huge potential for transformation that could offset the cost- / time-related impacts of increased overheads in the long run
Sourcing models				
Service providers				
Locations				
Governance				
Contracting				
Comments	Significantly increased overheads across most components of global services strategy – leading to massive timeline and cost pressures, especially in the “teething” phases	Almost all components offer attractive opportunities for transformation of service delivery – in most cases, this transformational push is in the same direction as ongoing/ planned transformation (e.g., increased leverage of technology or spurt in delivery from Europe)	Notable push towards consolidation – especially in service providers and locations portfolios. Similar to the “Opportunities for Transformation”, GDPR accentuates the push towards consolidation in provider and locations portfolios that was already being witnessed	

“You don’t need to fear GDPR; it is a key to create a culture of secure information technology.”

– McAfee

“Although GDPR may pose challenges, it provides opportunities for improving customer trust and fueling innovation, reliably and responsibly.”

– Denodo, data virtualization software company

Conclusion

With less than a year to go before the Data Protection Directive 95/46/EC is replaced by GDPR in May 2018, organizations should already have embarked on the preparation and implementation of the large-scale changes mandated by GDPR.

As organizations move ahead on their plans, they will need to keep the following imperatives in view:

- Be prepared to leverage **specialist expertise**, given the complexity of the regulation and high stakes (both from a financial and reputational perspective)
- Take a view across the entire **ecosystem of service delivery** (front-office / back-office, business units, functions, locations, and sourcing models)
- Disruption caused by GDPR will also offer **opportunities** for long-term transformation and consolidation of the service delivery organization
- Smart organizations will **orchestrate** the changes necessitated by GDPR compliance readiness with those caused by other disruptive forces (e.g., digitalization, automation, talent shortages, need to support increasingly complex services, and other macro-economic/geo-political/legal/regulatory environment changes), so that the net impact is additive, than opposite

The **good news** is that, for most large enterprises, the push from GDPR towards transformation and consolidation is in the same direction as their planned strategy for global service delivery.

In a second edition of this viewpoint, we will evaluate some of the above implications on global services delivery in more detail, e.g., transformation of offerings of service providers and impact of GDPR on service delivery across various industries. Keep watching this space for more!

We wish to thank the following experts for contributing their valuable perspectives on this topic:

- Bob Fawthrop, Director, Bob Fawthrop Associates Ltd.
- Kate Brimsted, Head of Data and Cyber Security, Commercial & Technology, Berwin Leighton Paisner LLP

Appendix

Key changes proposed by GDPR

While GDPR upholds the key principles of data protection, many changes have been incorporated to provide additional protection against data breach and attacks on data privacy.

Exhibit 3 summarizes the key changes proposed by GDPR over the existing Data Protection Directive, and rates the extent of changes in stringency levels across multiple aspects

EXHIBIT 3

Differences between Data Protection Directive and GDPR

Source: Everest Group (2017)











	Data Protection Directive Directive 95/46/EC	GDPR	Change In stringency
 Territorial scope	Applicable if personal data is processed within EU or by using the equipment located in EU	Will also apply to organizations established outside the EU, but involved in processing personal data of EU citizens to offer goods or services within EU	↑
 One-stop shop	Organizations are answerable to DPAs of the respective EU countries of establishment	Where an enterprise has an EU office, mandates single supervisory authority (lead DPA) for addressing data protection complaints across all EU member states	↔
 Consent	Personal data of subjects is attained by implicit actions, opt out boxes, and pre-ticked boxes	Consent by data subjects must meet rigorous standards and be freely given, specific, informed, unambiguous, and given by a clear affirmative action	↑
 Penalties	Penalties include civil sanctions, criminal sanctions, forfeitures, and fines up to EUR250,000	Non-compliance would invite fines up to 4% of annual global turnover or EUR20 million, whichever is maximum	↑
 Privacy by design	Data protection mechanisms are currently unregulated, with "privacy as an afterthought" being widespread	Requires inclusion of data protection into the designing phase of processing activities	↑

EXHIBIT 3 (continued)

Difference between Data Protection Directive and GDPR

Source: Everest Group (2017)

	Data Protection Directive Directive 95/46/EC	GDPR	Change In stringency
 Data protection officer	No mandate on appointment of DPO	Companies carrying out large scale processing of special categories of personal data are mandated to appoint a DPO	↑
 Controller-processor liabilities	<ul style="list-style-type: none"> Absence of a legal regime applying to service providers Controllers are generally not liable for downstream processing errors, if procedures were followed 	<ul style="list-style-type: none"> Service providers will have significant legal obligations Controllers are liable for processor violations. They must pay the fines, then sue the processor for damages 	↑
 Breach notifications	<ul style="list-style-type: none"> No express legal obligations to report data breaches It, however, indicates that serious breaches should be reported 	<ul style="list-style-type: none"> Organizations must report "high risk" breaches to regulators and data subjects within 72 hours of becoming aware of the breach 	↑
 Data subject rights	<p>Data subject rights are limited:</p> <ul style="list-style-type: none"> Right to erasure is limited and suppresses results of internet searches only Right to access is ambiguous without any obligations on controller regarding period and format of data to be provided to subject Absence of right bestowing powers similar to data portability 	<p>Data subjects have broad, legally enforceable rights, including:</p> <ul style="list-style-type: none"> Right to have personal data erased Right to demand a stop on processing of personal data Right to access and rectify personal data Right to get a copy of personal data in a standard, portable format 	↑
 Binding corporate rules (BCR)	BCR requirements were laid down separately in a series of working documents published by Article 29 working party	Official mention of requirements for BCRs, which can be used to transfer data internationally in case of absence of adequacy decisions	↔

Glossary of important terms used in the document

Term	Description
B	
Binding Corporate Rules (BCR)	Set of rules drafted to allow multinational corporations and group of companies to execute inter-organizational transfer of personal data outside the borders EU
BCS	Internationally-regarded foundation providing certification in information security principles
C	
CREST	CREST is an approved accreditation body that certifies its member companies on ability to handle sensitive and personal information
D	
Data controllers	Enterprise or organization that decides the purpose for which any personal data is to be used and the way in which the data is to be processed. Data controllers are enterprises in the context of this document
Data processor	Third parties that process the data on behalf of the data controllers. Data processors are service providers or GICs in the context of this document
Data Protection (DPA)	Authorities bestowed with the responsibility of ensuring compliance to data protection authorities
Data Protection (DPD)	The current regulation in European Union to govern the protection of personal data of EU citizens. DPD would be replaced by GDPR in May, 2018
Data subject	Any person whose personal data is being collected, held, or processed
G	
General Data Protection Regulations (GDPR)	New privacy protection regulations adopted by European Parliament in April 2016. The regulations would come into full effect in May, 2018
Global In-house Centers (GIC)	An entity within a multi-unit organization tasked with supplying the different business units within the organization with specialized services (e.g., finance, HR, IT services, facilities, logistics, and sales transactions) on the basis of a Service Level Agreement (SLA)
H	
Hybrid models	A sourcing model in which the service delivery is distributed between onshore, nearshore, and offshore delivery centers


Glossary of important terms used in the document


Term	Description
I	
ISACA	International professional association focused on IT governance, providing certifications in information system governance, security, audit, and assurance
P	
Personal data	Data, including name, ID number, location information, online identifier, or specific factors such as physical, physiological, mental, genetic, economic, cultural, or social identity which, alone or considered together, can lead to identification of an individual
S	
Service provider	Third parties that process the data on behalf of the enterprise or provide other services to it
Shared Services Center (SSC)	An entity in an organization responsible for handling and execution of specific operational tasks such as accounting, payroll, legal, and human resources; services typically shared by multiple business units, functions, or geographical subdivisions of the organization
Subprocessors	Third parties that process data on behalf of the data processor
Subject access request	A written request made by the data subject to the data controller, to access the data stored on them

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 empowers 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.


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):

 Eric Simonson, Managing Partner
Eric.simonson@everestgrp.com

 Julian Herbert, Vice President
Julian.herbert@everestgrp.com

 Anurag Srivastava, Vice President
Anurag.srivastava@everestgrp.com

 Chirag Bhatia, Senior Analyst
Chirag.bhatia@everestgrp.com