LTI
Let's Solve

GDPR: After
25th May 2018

Author
Ramees Mohamed

A Larsen & Toubro Group Company

Introduction

General Data Protection Regulation (GDPR) is a regulation that intends to protect the personal data and privacy of EU residents. It's a legal framework that sets guidelines on data collection and processing of personal information of EU residents within the EU.

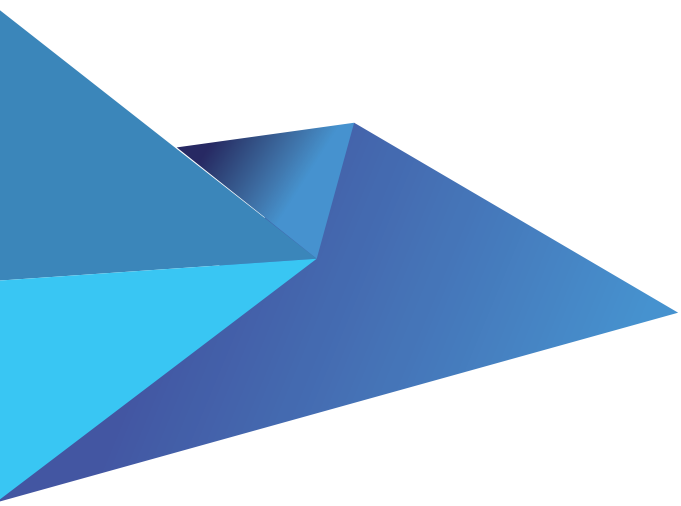
GDPR is the most stringent data protection regulation existing currently, and will set the tone for data protection laws around the world in the future. GDPR is all set to be the "new norm" in the digital world.

With few days into GDPR being effective we have seen little changes on the ground. Let's look at how things may shape up in the next few weeks and months from the perspective of companies and EU residents.

What changed between DPD and GDPR

There already is a regulation in the EU in force currently, which is called Data Protection Directive (also known as Directive 95/46/EC or DPD). This was a regulation adopted by the European Union in the year 1995 to protect the privacy and protection of all personal data collected for EU citizens, especially, as it relates to processing, using or exchanging such data. The Data Protection Directive is superseded by the General Data Protection Regulation (GDPR), which was adopted by the European Parliament and European Council in April 2016, and has become enforceable from 25th May 2018.

Although many of the underlying principles remain the same, the fact remains that GDPR's scope is far more comprehensive and wide-reaching than DPD. This means that even businesses based in the EU, which are already following DPD, will have to amend their data protection policies accordingly, else potentially face serious consequences.



The new regulation expands upon previous requirements for collecting, storing and sharing personal data, and requires the subject's consent to be given explicitly and not checked-off by default.

GDPR also widens the definition of "personal data", thereby, including online identification markers, location data, genetic information and more.

Under GDPR, organizations are mandated to notify a data breach within 72 hours of becoming aware of the breach; the notification in DPD regime was more of an encouragement than a requirement.

GDPR places explicit accountability on companies to prove that they comply with the regulations by conducting regular internal staff trainings, internal compliance audits, detailed documentation and traceability of all data subject rights requests.

GDPR mandates appointment of a Data Protection Officer for organizations processing large amount of EU data, which is not the case for DPD.

Heavy penalties for non-compliance – the DPD mandates a penalty of up to 500k Pounds or 1% of the annual turnover, however this has been significantly increased in GDPR to up to 20 million Euros or 4% of the annual global turnover.

For EU-based companies already complying with DPD, adopting GDPR will be an incremental change. However, with a wider scope of GDPR covering companies outside the EU servicing large number EU residents, compliance will be an uphill task.

Corporate Perceptions: How will companies react

With the lackluster response, preparedness and spending that was observed over the past few months on GDPR, many of the companies would have taken a risk-based approach depending upon their current data protection policy and risk appetite.

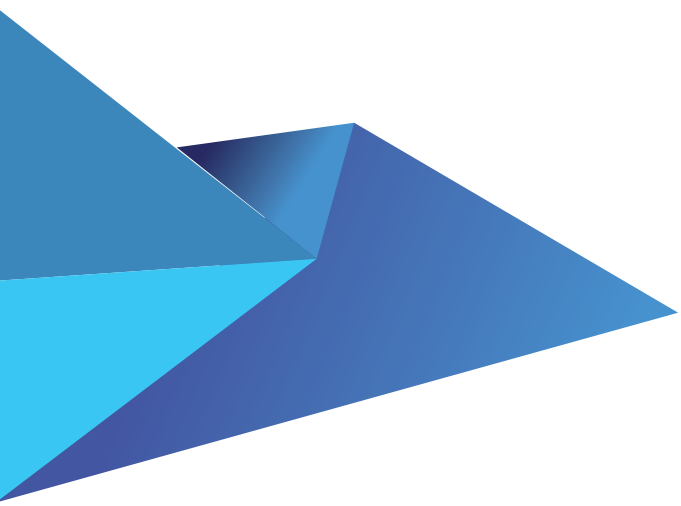
Most of the mid-sized companies might have done some kind of GDPR evaluation, brainstorming or assessment to ascertain what's their risk and exposure to privacy breach and penalties. The focus would have been to at least identify their most risky business processes and/or IT systems, and assess likelihood of a data breach and its potential impact. Some of the companies amongst these would have added additional checks and balances in their business processes to ensure that the breach likelihood score goes down significantly by bringing down their overall risk exposure.

Most companies would also focus on internal awareness of GDPR since this is a low hanging fruit, and would bank on more GDPR-trained staff to mitigate some of their risks. Almost all companies who have online presence would have reviewed and modified their policy agreements to add GDPR-relevant clauses in.

It would be interesting to see how many organizations just reduce/stop collecting data, where they perceive that the risk and cost of collecting and processing such data in a GDPR-compliant way, far outweigh the benefits it brings to their business. Example: Some retail stores may review their loyalty programs for effectiveness and business value it brings to them viz-a-viz the cost to re-architect their IT and business processes to comply with GDPR, and still bear risk-heavy penalties on breaches.

For companies based outside of the EU region but having large customer base in the EU region, getting compliant will be a steeper climb since they may not be compliant with DPD in the first place. DPD never impacted them since the older regulation was primarily targeted towards the companies based in EU.

This law will cause a sense of equilibrium, wherein data collection and tracking has almost become a new norm in the age of digital revolution. The likes of Alexa, Siri and Google Assistant will have to seek specific permission and declare if they are hearing and storing all conversations that we have in the interest of showing relevant advertisements.



Subject Rights Requests

GDPR has been in the news for quite some time and EU residents have been more than ever waiting for this regulation, and will feel a renewed sense of control and independence with regards to sharing their personal details and negotiating with their companies. There will be a sudden surge in the number of service requests coming in from residents to exercise their rights. There will be a group of people wanting to put a hold on all automated processing and decision making to regain the perception of control over their personal data.

The much talked about "Right to be forgotten"

A whole bunch of EU residents, especially senior citizens who were always concerned and didn't like the amount of personal data being captured and stored in the new era of digital world, would raise right to be forgotten requests.

As far as Britain is concerned, Britishers will be keen to exercise "the right to be forgotten", also because they will not be in EU effective March 2019, when Brexit comes into force. The UK would need to implement GDPR as a law separately in the form of a bill for it to continue with this law.

The right to be forgotten in some form, is existent since 2014 due to the European Court of Justice (ECJ) ruling and has been implemented by Google in its search results, which accounts for 90% of the search engine market in Europe. Out of the two million links submitted (720,000 requests) to be removed Google has removed around 43%. Google has been able to deny deletion of the remaining links attributing it to other legitimate reasons like safeguarding public interests.

Consent Requests

Contrary to the general belief, there may not be a huge burst of specific consent requests to the data subjects, as to provide services as per the agreed contract with their customers, organizations don't need to get specific consents.

But data subjects can get some thoughtfully made requests outside the scope of their service contracts. Change achieving to getting Data Subjects consent on these requests will be difficult unless the data controller is able to logically relate these additional data processing to improved and tangible benefits to the Data Subjects.

Settling in Period

As with any regulation or law, the first few months are learning lessons for all stakeholders. The data controllers will not be able to effectively manage the huge inflow of Data Subject Rights requests flowing in a timely manner. It will be difficult for data controllers to make decisions and implement many of the requests considering the multiple conditions and scenarios; unless the data controllers have already streamlined their process to the extent of clearly pre-defining these use-cases, their decisions and their implementation plan. For e.g.: In case of the right to be forgotten, what should be done with data that is archived in tapes and shipped to archival storage locations.

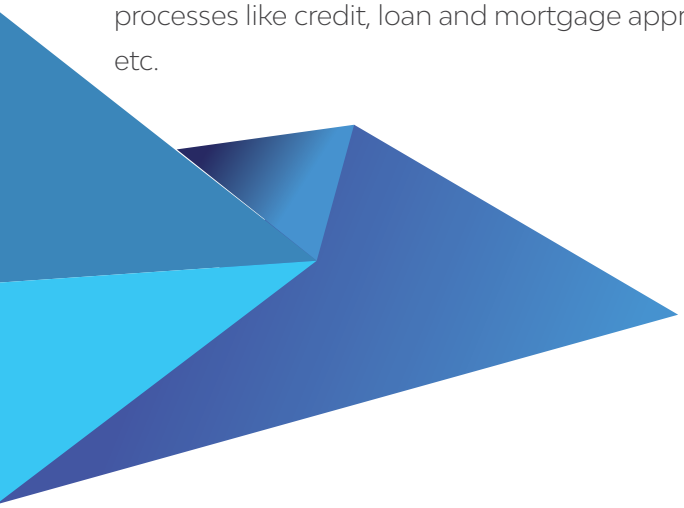
For doing this, we will need to ship back these tapes, extract the data in a separate storage location, identify the data subject's information and delete, archive the remaining data back again into tapes and finally ship it back. Does this constitute reasonable steps, use of available technology and cost of implementation?

The legal team in the data controller's and data processor's office will be pre-occupied, trying to address such questions from their various departments. This turbidity will remain until a clear code of conduct, as stated in article 40 of GDPR, is published by the member states and the supervisory authorities.

Data Equilibrium

GDPR regulations need humans to play a prominent role in privacy matters. The AI and machine learning algorithms will need to be tweaked for human inputs, so they are sensitive towards data subjects consent before using any identifiable attributes. This will need the algorithms to be more mature, these systems will not be compliant immediately starting 25th May this year. As a result, we can expect slowness in automated processes like credit, loan and mortgage approvals, etc.

In all these years of digitization and automation, we have evolved from manual processing to expedited processing, learning, improvization, automation and innovation. In this evolution, we have maximized our data capture affinity and increased hunger for accumulating more data anticipating future use. The GDPR regulation is in a way trying to find an equilibrium between uncontrolled data accumulation to rights of privacy and control over individual data.



Conclusion

Although GDPR is a much talked about and debated subject globally in the past several months, there seems to be little preparedness from organizations to implement this in a comprehensive way. The articles are broad policy outlines which further need to be strengthened by procedures, control mechanism and IT systems, which organizations are still working through. The rest of the months in 2018 will be a learning phase with regulators and supervisory authorities tightening the grip on GDPR by early 2019. So organizations can still catch-up and be on the right side of the line by becoming compliant at the earliest.

Ramees Mohamed
Deputy Analytics Lead, LTI

Ramees is a Certified Big Data Architect and has 20 years of Industry experience in Solution Shaping, Architecture and Implementation across Industry Verticals for Fortune 500 clients. His focus area is on Data & Analytics, Business Intelligence, Big Data Analytics and Master Data Management. He has played various key roles in multiple data-driven transformational programs across Life Sciences, Consumer Goods & Services, Insurance and Public sector domains. He has also played a role of SME multiple times to help clients in conducting technical assessments of their BI and Analytics program and establishing their Performance Engineering Practice.