LTIMindtree

Point of View

GDPR Assurance

More Than Testing For Compliance

Author
Brijesh Prabhakar
Business Head - Assurance Services

GDPR in Context

In the last 12 months, a health insurance company agreed to a settlement in excess of $100M in connection to a data breach that affected more than 80 million of its customers. Approximately, 200 million records belonging to American citizens were found on a well-known Cloud services infrastructure provider, without password protection. In another case, a popular email service was targeted to obtain the personal data of its users – it is estimated that over one million records may have been compromised in one hour!

The line between the virtual world and the real world has blurred considerably over the past few years. The ubiquitous nature of personal data, be it for a banking transaction or an online purchase, makes it easy for a determined hacker to compromise some of the best protected systems. This tramples on the rights of citizens who submit personal data to 'Data Controllers' and 'Data Processors', with an implied understanding that their personal data will be protected.

European Union's General Data Protection Regulation, GDPR, aims to change all this. It explicitly calls out the nature of the data to be protected, the rights of EU residents and the controls that are required to implement them. No longer can the protection of personal data be an afterthought to be retrofitted onto existing applications. The GDPR introduces and mandates a strict organization governance model to protect EU residents' rights. It also provides a framework for individual EU countries to implement their own rules based on the articles contained in the Regulation.

GDPR Assurance: Ensuring you are compliant

As the clocks tick down for organizations to become compliant before the 25th of May, 2018, the complexity of meeting these mandates are becoming clear. This is more than just an act of keeping all the data under lock and key or having a faster way to process key citizen rights such as 'right to access', 'right to erasure', 'right to data portability', etc. or the ability to notify a breach in 72 hours.

While the strategies may vary based on the industry / domain, one thing is clear – the ability to confidently state that you are ready for the GDPR demands thorough testing of the controls, enabling mechanisms for segregation of duties, automating checks, provisioning of an instant alert mechanism for breaches, etc. For an enterprise which consists of hundreds of applications, thousands of databases, and innumerable data interchange services – the ability to manually test and certify can be an all-consuming task.

Data in an enterprise is not static – once created, it flows, transforms and spreads throughout an application ecosystem. Despite many years of creating Master Data Management Systems and trying to protect personal data, the proliferation of personal information represents a huge challenge to become GDPR compliant.

LTIMindtree's GDPR Assurance platform considers the following:

Test for coverage of PII inventory – LTIMindtree's GDPR Assurance platform can scan through multiple databases, unstructured data, and file systems to validate the PII inventory that an organization may have done as part of an initial assessment.

Flag high risk repositories – Given the all-inclusive nature of GDPR, it is necessary to be able to identify data repositories that hold high risk information such as credit card numbers, national id numbers, bank account numbers, etc. LTIMindtree's Assurance platform can score high risk areas in an automated way. This can act as an input to application SMEs to determine if the flagging was correct.

Test data flows and data profusion – The nature of transference of data needs to be addressed. Data will flow within an organization and also be interchanged with external entities (Data Processers). This data profusion needs to be identified to create mechanisms that are required to notify in case of a data breach, when the data is transformed or transferred.

Test for Rights of Citizens – The GDPR outlines eight major rights – all of which make not only the protection of data important but aligning it to these rights equally important. These rights may impact functionality of an application or reduce the features that a customer can use. For e.g. if a customer refuses the permission to share his / her email, it may impact notifications of services or worse, functionalities - such as a password reset workflow. Many self-service options may become redundant.

Simulation of data breach – As part of testing the controls, it is important that real life simulations are conducted. The process to automatically notify Data Protection Officers, Regulatory Board, and citizens must be simulated in case there is a breach in production.

Application performance – Building controls around data and its transfer may impact application performance. For e.g. if previously stored plain text data is now encrypted, the extra step to unencrypt may degrade the application's responsiveness. This may be especially true if an application uses a large amount of such data in its transactions.

Test for Accounting and Data Retention Regulations – Global organizations need to comply with security and financial regulations such as KYC, AML, etc. In this scenario, it is necessary for organizations to test these compliance needs along with the citizen's rights.

Test for building compliance into the SDLC – The GDPR mandates both the software and the process for developing software needs to be compliant with data protection regulations. Compliance needs to be built into the SDLC rather than retrofit onto the application, after it has been built. LTIMindtree's early warning API can identify new data fields that have been added to capture PI data as part of the application build process. This report can be downloaded and provided to the DPO or an audit team on demand.

Test for security – OWASP vulnerabilities are one of the main reasons for data breaches, thus making it essential that applications are hardened against them and certified by penetration tests and segregation of duties testing (authentication & authorization tests).

About the Author

Brijesh Prabhakar

In his 19 years of experience, Brijesh Prabhakar has led and delivered global transformation programs for organizations such as GE, Walmart, ebay, AIG, Direct Line Group, and GM. Brijesh currently heads the Assurance Practice at LTIMindtree, where he is pushing the boundaries of Quality Assurance in the areas of Test Ecosystem Management, Digital Economy Transformation, Customer Experience, and Compliance Assurance. His views on Compliance Assurance are the outcome of his background in delivering PCI-DSS compliance for large Financial Services organizations, and pioneering work done in the space of payment systems for the blind.