Proceedings of the Second International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2018)
IEEE Xplore Part Number:CFP18OZV-ART; ISBN:978-1-5386-1442-6

Strategy and Solution to comply with GDPR

Guideline to comply major articles and save penalty from non-compliance

G.Priyadharshini
Research Scholar, PG & Research Department of Computer Science, Dr. Ambedkar Government Arts College, Chennai, India
sushpriya@yahoo.com

Dr. K. Shyamala
Associate Professor, PG & Research Department of Computer Science, Dr. Ambedkar Government Arts College, Chennai, India
shyamalakannan@gmail.com

***Abstract*— General Data Protection Regulation (GDPR) is no more buzz word and it sets new standard on security across globe. Every organization who deals with data started doing self-assessment to check how it has impact on their business and what are all the ways they can prepare themselves to comply with GDPR. Since 1995, Europe Union (EU) followed "Data Protective Directive" (Directive) on Data privacy. Fourth Industrial Revolution (4IR) has range of new technologies covering digital, artificial, biological and big data and impacting all discipline from aeronautical to economies and industries. Because of fast-moving technology and transformed individual and business behaviors, directive is outdated and is replaced with the General Data Protection Regulation (REGULATION (EU) 2016/679) Compared with Directive, GDPR is most ambitious one and it covers more operators under this act. The regulation completely changes the groundwork for how organizations can manage personal data of EU citizens. GDPR gives more control on Personally Identifiable Information (PII), Protected Health Information (PHI) or other sensitive information and imposes new rules on organization who manage and process PII or PHI. Objective of this white paper is to give broad overview of forthcoming GDPR and it doesn't focus on legal clause or penalty details. This covers the difference between Directive and GDPR, who are all covered under these new regulations. This also gives idea about consequences of the GDPR if an organization don't comply with GDPR and how organization to prepare themselves so that they can continue their business as usual without any impact and guide to avoid data breach and penalty.**

***Keywords*— GDPR, Directive, EU Data Privacy, Data Security, PII, PHI**

I. INTRODUCTION

Data Protection Directive 95/46/EC which came into force in 1995 provide guidelines on processing personal data in EU. The increasing number of security breaches, data theft, globalization, rapid development on technological trend brought new challenges to protect sensitive information including PII and PHI. When GDPR is proposed in 2012, it has attracted huge amount of attention among organization that are controlling, processing and using personal data of EU. After 4 years of discussion, GDPR framework was adopted on 8th April 2016. To adopt the new changes, organizations need time to align with new regulations. To transform current transaction to GDPR compliant, two year transition period is considered and decided to come to effect from 25th May 2018. This will supersede current directive and widen stakeholder coverage. GDPR have been influencing decisions by the Court of Justice of the EU. Organizations have been frustrated by the increasing lack of harmonization across the Member States, despite data flowing increasingly without boundaries. Globalization and increased data forced to have restriction on data processing. Global players want to implement GDPR quickly, even if that meant that some of the detail is left for later. Adoption of the GDPR marks a milestone in data protection laws in the EU and creates huge impact on data processing across the globe [3].

Figure 1 Focused areas for GDPR

There are 99 articles in GDPR which are grouped into 11 chapters. To comply with GDPR, all impacted organizations to do more changes and it requires time, effort and changes in process and work. The most significant changes are listed below as per GDPR Article [9]

- As per GDPR, 2016/679, Chapter VI, Section 2, Article 33(1), personal data breaches must be reported within 72 hours. If data breach leads to high risk for Data Subject (Data Subject mentioned in the GDPR is the person whose data is being collected and/or processed), it must be communicated to data subject immediately [10]
- As per GDPR, 2016/679, Chapter IV, Section 4, Article 37-39, if an organization involves systematic monitoring of personal data, it must appoint Data

Protection Officer (DPO) for all public authorizes [11]

- GDPR gave several new rights to personal data which helps individual to alter the scope and information. Some of them are :
    - Right to be rectification (GDPR, 2016/679, Chapter III, Section 3, Article 16) data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. [12]
    - Right to be forgotten (GDPR, 2016/679, Chapter III, Section 3, Article 17), allows to delete data of individual if requested [13]
    - Right to data portability (GDPR, 2016/679, Chapter III, Section 3, Article 20) allows individuals to transfer their data from one organization to other without any hindrance [14]
- Individuals can request organization who controls or processes their data to know 'fair and transparent' information about data processing like contact details of organization, details of data transfers outside of EU, data retention period etc.
- Organizations must follow new constraint consent protocol:
    - consent from data subject must be specific
    - processing of children data (under age 13) must get consent from parents
- Processing of personal data revealing personal identity like biometric for unique identification, health related data including medical report , political opinions, racial or ethnic origin, religious or philosophical beliefs, and the processing of genetic data, concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. These can be exempted only if data subject has given explicit consent to process these data for specific purpose [15]
- Data privacy must be considered at initial stage (Privacy by default) of design and all stages of life cycle in data processing (Privacy by design) [16]
- Taking into account the nature, scope, context, data controller must implement appropriate technical and organizational measures to ensure its processing activities are compliant with the requirements of the GDPR.

II. PROBLEM STATEMENT

All organizations across globe that capture PII relating to EU citizens must comply with its provisions from May 2018. Any failure to comply with GDPR exposes organizations to fines of as much as €20 million or 4% of global turnover— whichever is higher. The increasingly digital nature of business and data sources from various formats makes it more difficult to monitor individual customer's PII across an organization.

Organizations which are dealing with EU data are more concern about their business continuity, impact on their availability to use data related to EU customers and individuals. Since GDPR has come to effect from 25th May 2018, organizations are prepared to be compliant otherwise it will have huge impact on their business and end up with paying penalty. Organizations are comply with various measures of GDPR (important one are listed in Introduction section) and its territorial scope are increased, all businesses handling PII, PHI or similar personal data on people residing in the EU are subject to these regulations, regardless of where the business is located.

Compuware survey [18] also highlights below points as part of their recent survey. Organizations are facing challenges to meet GDPR. Some of the challenges from data governance point of view are:

- Define PII to include everything from customer email addresses and tax IDs to their hobbies and social media posts.
- As part of GDPR, data processing organization must get customer permission to use PII in application testing. Some of the organization who are doing application testing on PII are not having clear plan to comply on this mandate
- Considering data complexity of 4IR, organizations not even know where data resides in their system.
- 94% of organizations are processing EU data and only 60% are having detailed plan for GDPR compliance.
- One third of organizations don't clearly understand what GDPR is and how it is going to impact their business. Some of them not sure whether their business to comply with GDPR or not

Figure (2) gives survey report conducted by Compuware on challenging areas for organization to comply GDPR [17]

Figure 2 GDPR Challenges

III. LITERATURE REVIEW

Bert-Jaap-Koop et al. [19] clearly specifies the problems with European protection law. The main objectives of data protection law are based on three fallacies. The first fallacy is the belief that data protection law enables individuals to control their data and restrict the data flow, which it cannot. The second problem is that the reform simplifies the law, but in reality, the new law makes more complexities to become compliance with all regulations. The third fallacy is the assumption that regulations are more elaborative and covers all area , but these regulations are stretches data to the point of breaking and the original meaning of data is lost in the books.

Resolving Conflicting International Data Privacy Rules in Cyberspace [20] explores the divergences in approach and substance of data privacy between Europe and the United States. The article concludes with logical category of strategies and partners to develop cooperation across the globe and ensure there is no data leakage when personal data are transferred to other geographies.

The EU Data Protection Directive: An engine of a global regime computer law & Security Review [21] explores a unique form of legal globalization, in which one jurisdiction induces other countries to adopt similar legal mechanisms, without coercion, taking advantage of ignorance or abusing political power.

This research paper covers important articles in the area of territorial scope, data privacy, individual rights, required data governance for any organization to comply with GDPR and solutions which help to avoid penalty for any breaches or non-compliance.

IV. PROPOSED SOLUTION

When organizations comply with directive regulation, it must obviously mandate to comply with GDPR as well. There are few organizations which may not come under current scope of directive, but because of increased scope of PII, territorial scope and rights of data subject, they also need to comply with GDPR. If an organization processes PII in EU, GDPR will apply to this organization. Processing includes operations on personal data including data collection, storage, transfer or purge. If an organization establishes outside of EU and offering goods and services to EU data subject or monitoring behavior of EU data, then these organizations must also comply with GDPR. It applies to both controllers who control personal data like cloud and processor who perform operation on data. Organization need to know the following and align with regulations to comply GDPR

A. Roadmap for GDPR

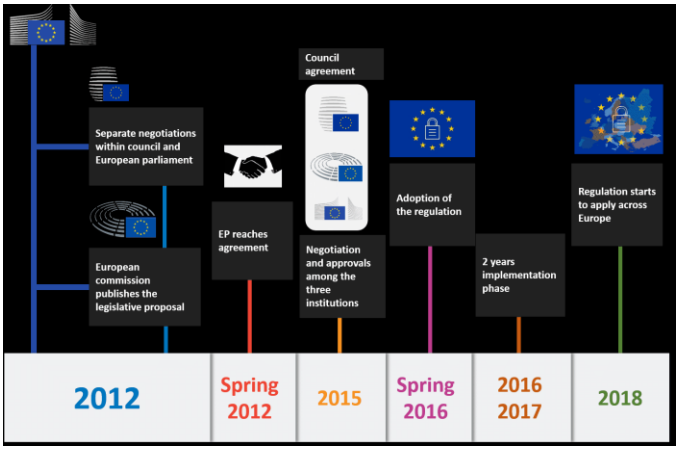

Figure 3Roadmap for evolution of GDPR

B. Territorial Scope

An organization outside the EU which is targeting consumer in EU will come under GDPR where as they were not covered in directive. Data controllers and processors whose processing activities related to goods or services, data monitoring must comply with GDPR. Offering goods and Services includes having access to website, languages or currencies used in any member stage of EU. When individuals are tracked on the internet by techniques which enable to predict personal preferences, it will come under "monitoring behavior"

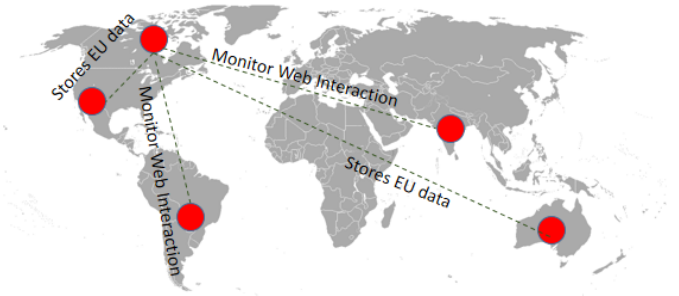

Figure 4 Territorial Scope

C. Identify and assess data and data protection

Once geography is understood and their scopes are defined, it is necessary to identify volume, velocity of personal data and

its corresponding risk to protect them. Discovery of personal data and its risk assessment to be completed across wide range of tools and technologies. These tools will help quickly spot, monitor and provide data security for PII across all types of sources and data types. It is important to protect critical data source across the organization and reduce risk because of 4IR including cloud and Hadoop. It is also important to have baseline the data and monitor regulatory compliance, user behavior, data access and movement. Any suspicious behavior, unauthorized access or violation of privacy or industry regulations must be identified with right tools and immediate action must be taken if there is any deviation from compliance regulations. Detailed visualization and audit report for location, risk, protection, value and access of regulated data must be available through tools.

D. Holistic approach for data definition and Data governance

For effective data governance, holistic approach across organization must be taken by bringing together all data. Define policies, identify all internal and external stakeholders, and connect all data insights together to govern in scope data for GDPR compliance. It is also important to interconnect all products used in various business units. By integrating all products with the solution that organization uses, it enables to give whole organization the technology that is needed for successful data governance program. Data stewards play commendable value to organization by operating complex data environment. The right tool must be used which help stewards to discover the understanding from requirement and identify what is needed from data. Data governance tool can bring together all constituencies to enable teamwork up and down data governance organization among team members.

E. Control and purge data – Prevent unauthorized access

In an organization, many users will have access to various systems and database across geography. Most of time, access will not be revoked after completion of scope. There is a need to have defined user access management matrix that governs user access and regular review should be done so that there will not be any obsolete access which are no more required. Periodic de-identify, de-sensitize and anonymous sensitive data from unauthorized access for all users and systems. Data masking is one of general approach to protect sensitive data and for de-sensitize. By combining persistent and dynamic data encryption organization will have complete data protection for their data and compliant to GDPR. Data monitoring and control will help to restrict data growth in production databases and retire legacy applications, while managing retention and retaining access to business data.

F. Master data Management and 360 degree data view

The single customer view is best way for organizations since it helps them create the best possible customer experiences by collecting data from all required sources and manage from one location. With the introduction of the GDPR, the single customer view becomes even more relevant. For GDPR compliance, organizations need to quickly identify all data organization hold about data subject regardless of location or system. Personal data must be managed from central location, data from all location linked with application, data processing, control and monitor can be applied in a consistent and efficient way. Master Data Management (MDM) is not only used for consolidation and comparison, it is also resolve solution for below

- Ability to acquire data from various sources like third party system, cloud or within the organization quickly.
- Able to understand data pattern and validate date for improved quality and suggest required correction on data
- Reliable and trusted data view can be created and data can be delivered in secured protocol for any operational and analytical purpose.

V. EXECUTION APPROACH

An organization can follow below four stage process to prepare GDPR compliance. The stages are mentioned in Figure (4)

Assess: Current model of organization, technology landscape, policies and procedures must be analyzed in this stage. This will help to identify gaps on existing system

Report: This stage focuses on identifying loophole in the current system and missing processes to comply and get buy-in from management for funding and it must be reviewed with experts and legal to ensure new system will meet any regulatory requirements

Remediate: In this stage, new process and policy must be established and new systems to be implemented on demand. Any old system which are no more required must be decommissioned and system integration to be validated with new architecture. Necessary changes to be done on documents, training and awareness sessions to be conducted for user group as per their scope.

Operate: The new system must go operational before GDPR roll out and all business continuity, disaster recovery and fall back plan must be in place. Through regular governance and maintenance, process improvement, continuous improvement is required even after system stabilization. The new system also need to consider future growth of data and technology development and must be scalable at least for short duration

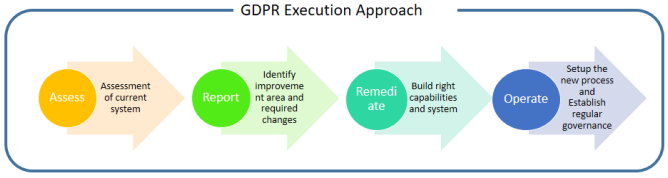

Figure 5 GDPR Execution Approach

To comply GDPR, most of organizations require change in strategies, policies and procedures, systems, redefined roles and responsibilities. In this transformation, business not only

required tangible changes but also cultural business changes. Every organization must prepared on these areas

Commitment and approved budget must be supported by board or top management of organization. Management must aware that cost for data compliance is less than cost for data noncompliance. The transition must have holistic organization wide approach to be successful. If an organization doesn't meet GDPR, its brand image will be damaged, paying more as penalty and have huge impact on economic sanctions

Identifying right person or team from all business unit of organization is the major step in this exercise. When an organization has best dedicated team, it can leverage all available accelerators in the organization and build new assets for the organization to meet GDPR. The teams have to educate themselves as well as educate the organization. If there is a need to hire DPO as per regulations, it has to be done quickly as DPO can also guide the team.

It is important to create data landscape map to cover all business units of organization, as data can be scattered across various platforms and systems within the organization. When organization deals with data, it is important to classify whether it belongs to data controller or data processor. Data landscape must help organization to identify where impacted data are stored within the system, which are all having access to these data and Meta data about data subject. Data quality, data protection policy and security controls must also be taken care and define procedure for notification to data subject.

Once data map is defined, it has to be combining with GDPR expertise. This helps to define policies, procedures and process to find any non-compliant areas. Once gap analysis is done for non-compliance data, necessary action can be taken as per risk. There may be some area where the organization many not have sufficient knowledge or bandwidth to bridge the gap. In such situation, where there is no capacity to solve internally, organization need to hire or outsource to experts or external agencies so that organization will be GDPR compliant.

There are numerous tools available to compliant on GDPR. By analyzing more than 60 tools, below are recommended for critical areas of GDPR such as security, Assessment, Data Governance , Data Management and User consent

A. Security

Table 1Seurity Tools

NAMEOF THE TOOL	KEY FEATURES
The Absolute Platform	It give an end-point security solution which is connected to every end point and helps to discover sensitive data and to identify the risk
Actiance Platform	The Actiance Platform is a unified platform designed for compliance across communications and social channels and gives users insights into what is being captured.
Alien Vault USM	Helps to detect data breaches, monitor data security, and document the compliance readiness
DB Networks	DB Networks provides artificial intelligence based database security for data base discovery, insider threat protection, and deep SQL analysis.
Egnyte Protect	Egnyte transforms businesses via smarter content that allows organizations to connect, protect, and unlock value from all of their content.

B. Assessment, Data Governance and Data Management

Table 2Seurity Tools

NAMEOF THE TOOL	KEY FEATURES
Collibra	This is useful to automate data management process, deliver transparency and for effective data governance between organizations.
BigId	BigID software assists companies in securing customer data and satisfying privacy regulations like GDPR. It performs Consent management to show that enforcing customer content regulations are enforced for personal data collection
Ave point Privacy Impact Assessment system	This tool helps users to assess progress with GDPR compliance and track the progress over time.
BMC discovery for Multi Cloud	This provides solution to automate asset discovery and application dependency mapping to give users a complete view of data center assets, multi-cloud services, and their relationships.
BWise GDPR Compliance solution	BWise helps to build holistic data view, data control and compliance in all parameter. It also helps align change management process along with rapid growth of business.

C. User Concent

NAMEOF THE TOOL	KEY FEATURES
Consent Cheq GDPR Compliance development kit	This tool is a solution for user consent and compliance. which is a fully integrated set of software tools, cloud API, and dashboard services with model compliance forms to give your enterprise a solution for quickly building, testing, and optimizing processes for GDPR compliance.
Consentua	Consentua is a consent management tool that helps organizations in achieving data protection compliance for regulations such as GDPR.
Evidon universal consent Platform	When an organization faces challenge to steamline digital governance, this will be right tool and it simplifies the governance.
PrivacyPerfect	This tool provides assessment, processing, breaches, dashboards, tools especially designed for chief privacy officers, reports, legal processing grounds, and graphical overviews.
Salpo GDPR compliance assessment tool	This tool helps businesses to grow quickly with latest technology adaption, CRM and mobile solutions. This is also useful for multi vendor management when development work is done by more than one vendor.

VI. Conclusion And Future Work

Once GDPR is implemented, organization will have varying impact on the way they do business, policies, procedures and hierarchy within organization. Organization must make sure those key stakeholders are aware of the changes and impact of GDPR. Management team must have knowledge on underlying reason for this regulation and need to appreciate this move. Data without knowing its source and usage are expensive after GDPR. Organization must document the details of PII they hold, its source and its flow. Organizations need to review their communication policy, privacy notices and ensures they send notification for all changes made on personal data to right data subject. They also need to have mechanism to communicate any breaches within 72 hours.

Individual rights of data subject must be covered in organization procedure to make sure it is possible to make changes upon request, delete the data and transfer to other parties. Updated procedure must enable to handle data subject request within given time period and able to share any additional information.

Consent from individual including child must be followed to align with GDPR. Organization must review how to seek record and manage consent from data subject and decide whether it requires any changes to comply. Since children under 13 are also covered, the system must allow verifying individual's age and obtaining parental or guardian consent for any data processing task.

Organization must make sure it has the right procedures in place to find any security breach and able to detect, report to relevant stakeholders. On need basis, organization must appoint DPO to take ownership for data protection and compliance.

As next step, need to identify how to restrict data breach from network through improved process and tools implementation. Organization to be comply with GDPR, identification of right tool for various activities including master data management, data protection and masking, breach notification, consent declaration and privacy notification should be analyzed and recommended guideline is required for all type of organization.

References

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[2] https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation#
[3] http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf
[4] http://cdn2.hubspot.net/hubfs/659257/uk_site/resources/white-paper/white-paper-gdpr-en-uk.pdf
[5] http://www.oracle.com/us/gdpr-oracle-cloud-apps-4070546.pdf
[6] https://www.salesforce.com/content/dam/web/en_us/www/documents/white-papers/gpdr-fact-sheet.pdf
[7] https://www.verisec.com/wp-content/uploads/2017/11/WP_GDPR-Guidelines_MC.pdf
[8] https://www.clearswift.com/sites/default/files/documents/Whitepapers/Clearswift_GDPR_Whitepaper.pdf
[9] https://gdpr-info.eu/
[10] https://gdpr-info.eu/art-33-gdpr/
[11] https://gdpr-info.eu/art-37-gdpr/
[12] https://gdpr-info.eu/art-16-gdpr/
[13] https://gdpr-info.eu/art-17-gdpr/
[14] https://gdpr-info.eu/art-20-gdpr/
[15] https://gdpr-info.eu/art-9-gdpr/
[16] https://gdpr-info.eu/art-25-gdpr/
[17] https://www.cioinsight.com/security/slideshows/cios-are-concerned-about-the-impact-of-the-gdpr.html
[18] https://resources.compuware.com/research-improved-gdpr-readiness-businesses-still-at-risk-of-non-compliance
[19] International Data Privacy Law, Volume 4, Issue 4, 1 November 2014, Pages 250–261,https://doi.org/10.1093/idpl/ipu023
[20] Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 Stan. L. Rev. 1315 (1999-2000)
[21] Michael D Birnhack The EU Data Protection Directive: An engine of a global regime computer law & Security Review volume 24, issue 6, 2008,pages 508 -520.