A Systematic Approach to Ensuring GDPR Compliance: Key Action Items for Telecom Operators

Abstract

The General Data Protection Regulation (GDPR) is all set to come into force across the European Union (EU) in May 2018. Harmonizing 28 national legislations into a single continent-wide directive, GDPR marks the biggest overhaul of data privacy laws in the bloc in over two decades. Once GDPR kicks in, companies that service customers in the EU, even if located outside the region, will have to take appropriate technical and organizational measures to ensure regulatory compliance. Spanning over 99 articles, the law will impose strict standards for enterprises to protect their customers' personal data. Failure to adhere to these norms could potentially see businesses being slapped with heavy penalties, almost as high as 4% of their global annual turnover, according to PwC[1].

Protect customer data, or face consequences

GDPR will impact consumer-facing industries in particular, forcing companies to alter their business processes, revamp governance mechanisms, and even diversify revenue streams. The ramifications for the telecom sector will be significant, given that sensitive customer data form the backbone of its core operations. With the risk of network breaches increasing in the digital era, telcos will have to reimagine the way they collect, store, and analyze massive volumes of customer data in the post-GDPR landscape.

It is quite clear that wireless carriers will need to drastically revamp their operations in the wake of the new EU law. Amid declining average revenue per user (ARPU), fragile customer loyalty, and mounting competition from non-traditional, over-the-top (OTT) service providers, telcos cannot afford a compromise of subscriber data. As regulations being enacted in various jurisdictions hinder the efforts of mobile network operators to monetize client data for unearthing new revenue sources, non-conformance with GDPR could damage their goodwill, reputation, and customer trust. And, it is not just telcos that need to worry. Even third-party data processors will have to comply with GDPR.

Adapting to new rules

In order to ensure full compliance ahead of the GDPR deadline, telecom companies must comprehensively re-examine their business and operation support systems (BSS / OSS), as well as data management practices.

Customer consent is set to become a key pre-condition to storing and processing data throughout the entire supply chain of data processors. Carriers will need to completely erase any personally identifiable information (PII) of an individual subscriber, if the customer so wishes. Moreover, PII data sets must be made 'portable' and provided to users in a structured format upon request.

Accordingly, telcos will need to not only stay on top of their internal data warehouses, business processes, and reporting structures, but also of all their third-party service providers worldwide. This will necessitate a transformation of carriers' overall data management processes, beside major changes in their system architectures. As encrypting and/or anonymizing

all user data across enterprise systems assumes critical importance, mobile operators must also extensively test their front-end, online applications to minimize the risk of data breaches. In conjunction, they have to strengthen in-house data processing mechanisms through institutionalization of strict and multi-level access control for the personnel handling associated systems.

Overcoming compliance challenges

Implementing a wide-ranging, successful overhaul of OSS / BSS setups and data management processes will not be easy for telcos. It will require extensive planning, regular impact assessments, and adoption of new procedures. For instance, individual customers must be approached to seek explicit consent for usage of their data. Simultaneously, existing subscriber data needs to be reviewed, and any extraneous information must be minimized. Telcos will then have to tag the remaining data with personally identifiable information (PII), and evaluate it from a compliance standpoint. For accelerated user adoption, operators must also train their staff effectively on how to handle the revamped systems, and access and act on client data.

Apart from addressing these bottlenecks, telcos must revisit their existing strategies for cross-selling, up-selling, and customer outreach, based on a data-driven, personalized profiling of each customer. For example, carriers could, on the basis of consent, use PII to market tailored value added services (VAS) and data subscription plans to a customer roaming in and out of the EU. Implementing the consent mechanism for data monetization will be a complex and challenging affair.

Ensuring alignment

For telcos to be able to ensure a cost-effective and timely transformation of their data management workflows and network systems, they must systematically identify and prioritize the requisite changes. Even as their various IT vendors roll out individual applications compliant with GDPR, telcos will need to spend significant time and effort toward ensuring robust data governance and program management.

Overall, the GDPR conformance journey should involve a judicious mixture of top-down and bottom-up approaches, with all stakeholders being on the same page. It is therefore critical

to have a carefully designed, flexible compliance strategy, post identification of existing gaps in OSS, BSS, and audit trails.

To begin with, carriers should initiate a health check of their CRM systems to uncover vulnerabilities and deficiencies if any. A packaged GDPR solution that incorporates the essential elements of log management, audit trials, access management, consent mechanism, and vulnerability assessment may be implemented in this regard. Alternatively, telecom companies can look at implementing point solutions based on the order of priority and risk impact.

However, irrespective of the exact manner in which it is accomplished, GDPR conformance must be achieved in its entirety. Keeping this objective in mind, here are the key GDPR articles that telcos must thoroughly internalize to minimize any adverse impact arising from non-compliance:

Reference to the GDPR Act	Requirement	Solution	
Article 5	**Processing and Storing Personal Data**	Use personal data only for the purpose and time specified by the user, and process it lawfully, fairly, and in a transparent manner	Mask, encrypt, and anonymize all PII, depending on their exact usage and storage state
Articles 6, 7 and 8	**User consent**	Collect and process all personal data only after obtaining explicit consent from the user	Redesign processes linked to VAS and other data monetization strategies, in line with the user consent mandate
Article 12 to 22	**Rights of the data subject**	Honor the rights of the data subject with respect to right to access, rectification, right to be forgotten (data erasure), restriction of processing, notification obligation, data portability, and right to object including automated decision making (user profiling)	Implement a robust data lifecycle management framework involving data minimization and data access management, with built-in functionalities for easy data modification, portability and erasure
Articles 25 and 32	**Data protection by design**	Ensure data protection by design, and by default; carry out data protection impact assessments regularly	Leverage solutions such as data encryption, masking, and pseudonymization To shield subscriber data from internal threats, implement effective mobile device management (MDM) mechanisms for streamlining access for remote, off-site employees Promote role-based access to IT and data assets through enforcement of advanced identity and access management (IAM) protocols

Reference to the GDPR Act	Requirement	Solution	
Articles 25 and 32	**Data protection by design**	Ensure data protection by design, and by default; carry out data protection impact assessments regularly	Conduct a vulnerability assessment and penetration testing (VAPT) for all applications, and chalk out a business continuity plan (BCP) for each one
Articles 30	**Records of processing**	Maintain a record of all processing activities, covering specifically mentioned information on the processing	Prepare records of processing as a part of the GDPR assessment report
Articles 33 and 34	**Data breach**	Report data breaches within 72 hours	Build effective breach detection and notification mechanisms across internal systems
Article 35	**Impact assessments**	Conduct data protection impact assessments to identify risks to users, and also detail how such risks will be mitigated	Roll out an extensive compliance audit program for robust risk management
Articles 37, 38 and 39	**Data protection officers (DPO)**	Appoint a DPO to oversee the data security strategy and GDPR compliance	Appoint a DPO, and fix accountability or effective data governance

Looking ahead

GDPR will undoubtedly trigger widespread changes across the telecom landscape that could likely impact top-line growth and customer retention rates over the short term. Nevertheless, it represents a compelling opportunity for wireless carriers to fundamentally reimagine customer service, and make operations leaner and agile, through adoption of next-generation data management practices.

By protecting subscriber data, telcos will not only minimize the risks of financial losses but also inspire greater customer trust and loyalty that would pave the way for reduced churn and increased ARPU. And, with the data deluge only set to grow further, amid the IoT wave, GDPR compliance could help carriers prepare themselves well for the future.

References

[1] PwC, Press Release: GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey, (January 2017), accessed Sep 21, 2017, https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html

About The Authors

Geo John

Geo John is a Data Privacy Consultant with TCS' Cyber Security group. He has over 14 years of experience in the IT sector, primarily in the areas of data security systems. John works with TCS' clients, across various industry segments, to assess their data privacy setup and provide recommendations and design solutions in line with industry standards and company's privacy and compliance maturity.

Hussain Mirza

Hussain Mirza is a Data Privacy Consultant with TCS' Cyber Security group. Over 11 years of working with TCS, he has conducted assessments and audits to identify vulnerabilities with regard to data security and privacy risks for global organizations across various industries. Mirza is responsible for the development of controls and solutions that ensure privacy and security of sensitive and personal data.

Punit Nema

Punit Nema is Data Privacy and Security Consultant with TCS' Communications, Media, and Information Services business unit. With over 7 years of experience, he evaluates data protection requirement at applications, integrations, interfaces, and internal and external processes. Nema has worked on consulting assignments around building security solutions for TCS' telecom clients.

Contact

Visit the Communications, Media & Technology page on www.tcs.com

Email: global.cmi@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services I M I 10 I 17