WHITE PAPER

FIRST-MOVER ADVANTAGES OF IMPLEMENTING DATA PRIVACY IN COUNTRIES WHERE SUCH A LAW IS UNDER CONSIDERATION

With digital transformation accelerating across businesses in the last few years, the data being collected and processed is not only overwhelming and unsustainable but, most often, also sensitive and confidential in nature. It poses critical ethical and legal challenges such as unwarranted access to personal data, risk of a data breach and the financial cost it incurs – affecting millions of users, besides the geopolitical risks in a geostrategic environment. This necessitates data governance and data regulation, particularly in countries where a robust data protection law is still under consideration. Hence, proactive and overarching implementation of data privacy gives organizations a distinct advantage over their competitors in terms of improved data management, increased consumer confidence and becoming compliance-ready for the inevitable data protection regulation, among many other benefits.

Infosys®
Navigate your next

Overview

Data Privacy in today's digital age is considered as one of the fundamental rights of an individual, because of the sheer impact that data has on the social, economic, legal, political, and ethical aspects of human life. Every time you browse a webpage, or scroll through a social media post, check-in at a location, or interact with the Internet of Things (IoT) products installed in your homes – that information is recorded, processed, and sometimes even sold and resold without the individual's knowledge.

Data is an enterprise asset, and to ensure that it is used appropriately, robust privacy governance is required.

Myth about data - "The more, the merrier"

Digital transformation has brought about a phenomenal revolution in the way businesses operate – both in terms of delivering business value, as well as changing the overall business culture. And, at the heart of any digital transformation is data.

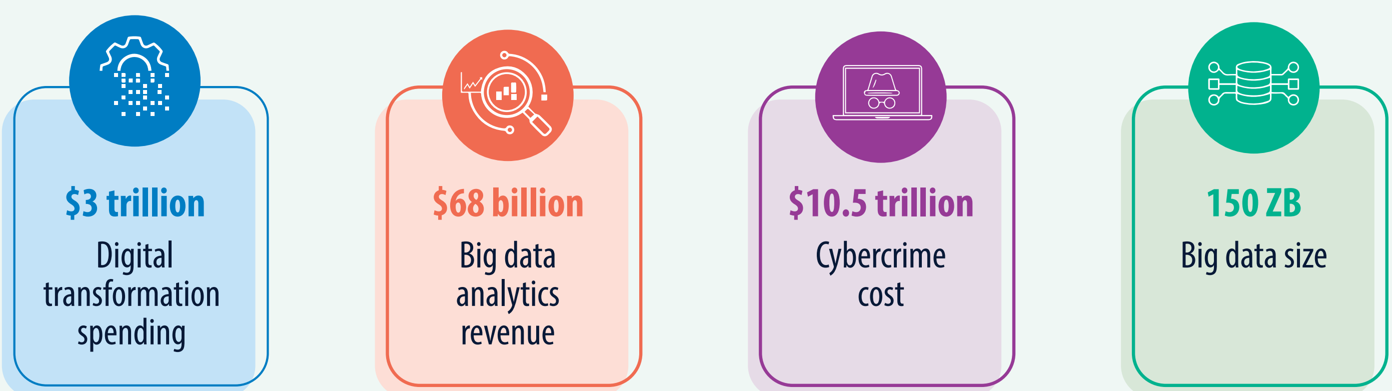
Data helps in understanding the consumer's pain points, predicting their behavior, optimizing operations and allows for more informed decision-making.

The amount of data created and consumed globally is said to increase by three times by 2025.[1] While the rapid growth of data, particularly after the advent of cloud computing, artificial intelligence, and the Internet of Things (IoT) has presented many opportunities, it has also brought to the fore the ethical and legal challenges associated with data – data privacy and data governance being the most critical ones. Consider the following:

- What do the massive and diversely sourced datasets being collected today comprise of? It is often personal data or personally identifiable information (PII). With more data being stored, there is a high risk of a data breach if left unprotected.
- What value does Bigdata hold if the data quality is poor? It not only results in inaccurate analytics and flawed decision-making, thereby impacting the trust in data, but is also an overhead with proliferating storage and processing, and an overall complicated data solution design.

While Businesses try to leverage the data that they hold to fuel digital transformation, they need to strike a balance between innovation and protecting the privacy rights of their customers.

Figure 1: 2025 Projections



Data breach impact: the high cost of the low price?

Businesses and governments can no longer choose to evade data privacy and underinvest in cyber security, as data breach incidents pose a risk not only to the privacy of individuals, but also causes disruption across the industry that has a wider economy-wide effect. About $600 billion, which amounts to one percent of the global GDP is said to be lost every year due to cyber-attacks.[2]

Most importantly, it poses a severe risk to the national security of sovereign countries, particularly in the wake of espionage campaigns, surveillance programs and communication blackouts. This is certainly a challenge to the global security community and has severe implications for the geopolitical landscape. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) had issued a warning of potential Russian cyberattacks affecting critical U.S. infrastructure days before Russia's invasion of Ukraine.[3]

According to the World Economic Forum, data fraud/thefts are the fourth biggest risk the world is facing today.[4] In contrast, the investment that enterprises and governments are making to address the digital threats is extremely low and unsustainable.

The top industries disclosing the highest number of data breaches are healthcare, retail, and finance.

Interestingly, data breaches can affect not only large corporations but also small and medium-sized businesses, with 60% of small companies reported to have been shut down globally within six months of a data breach.[5]

The now approaching digital future is going to be defined not just by innovation, but also by informed consumer choices and regulation. Furthermore, in a geostrategic environment where geopolitics and technology are intertwined inseparably, the government's preparedness and responses to cybersecurity attacks defines who gains and who loses. Hence, there is a growing need for data protection laws across the globe.

Figure 2: Key Data Privacy Risks that arise from Data Processing

Use-case1: Cloud Computing

Risks: Unauthorized access to data, Data breach, Data transfer over insecure channels

Impact: Reputational damage, Customer distrust, Compliance issues/Regulatory fines

Use-case2: IoT (Internet of Things)

Risks: Cultural/Behavioral profiling, Infiltration, Breach of confidentiality

Impact: Customer distrust, Sabotage of device's behavior, Disruption of operations

Use-case3: Big-data

Risks: Inaccurate data, Poor data quality, Data breach

Impact: Proliferating storage & processing, Flawed business decisions, Data abuse, Compliance issues, Complex design

Data protection law – keeping up with the digital age

With an objective to protect the personal data of individuals and strengthen their privacy rights, governments across the globe are enforcing data protection laws – such as the General Data Protection Regulation (GDPR) that came into effect in 2018 for the European Union, and the California Consumer Privacy Act (CCPA) in 2020. These laws have set an international benchmark in the pursuit of data protection, despite their shortcomings with respect to implementation. Other countries, such as United States, India, UAE, Tanzania, etc., are following suit.[6] Some of the countries have existing laws, which are either outdated or not comprehensive enough to address the challenges of the digital era.

Figure 3a: Laws that already existed before Digital age

Personal Information Protection and Electronic Documents Act,2000. Effect: Jan 2001 Canadian Human Rights Act, 1977

Personal Data Protection Act 25.326 (PDPA), Effect: 2000

Health Insurance Portability and Accountability Act (HIPAA), Effect: 1996
Fair Credit Reporting Act, Effect: 1970
Electronic Communications Privacy Act, Effect: 1986

Data Protection Act 1998

Privacy Act 1993

Information Technology Act, 2000
Information Technology Act, 2008

Russian Federal Law on Personal Data (No. 152-FZ) 2005. Effect : 2006

Telecommunications (Interception and Access) Act 1979 Privacy Act 1988

The Act on the Protection of Personal Information (Act No. 57 of (2003)), Effect: 2005
The Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003), Effect: 2007

Basic Law: Human Dignity and Liberty, 5752 - 1992
Protection of Privacy Law, 5741-1981

Figure 3b: Data privacy laws of the digital age

Personal Data Protection Law, Effect: Mar 2022

Protection of Personal Data, Effect: Jan 2022

Personal Information Protection Law, , Effect: Nov 2021

Russian Federal Law on Personal Data (No. 152-FZ), Effect: Jul 2006 Amendment Effect: Mar 2021

Singapore's Personal Data Protection Act 2012. Revised Effect: Feb 2021

General Personal Data Protection Law, 2018. Effect: Aug 2020

Protection of Personal Information Act. Effect: Jan 2022

California Consumer Privacy Act (CCPA) 2020, Effect: Jan 2020

Consumer Privacy Protection Act, 2018. Effect: Jan 2020

Privacy Act 2020, Effect: Dec 2020

Personal Data Protection Act 2019

General Data Protection Regulation (GDPR) 2018, Effect: May 2018

Personal Data Protection Act 2010, Effect: Nov 2013

Figure 3c: Data privacy laws in legislative process

- Resolución 159/2018 - RESOL-2018-159-APN-AAIP
- Personal Data Protection Bill, 2019
- California Consumer Privacy Rights Act (CPRA), Planned: 2023
  Virginia Consumer Data Protection Act, 2021, Planned: 2023
  Colorado Privacy Act, Planned: 2023
- Revision for Australia's Privacy Act 1988
- Digital Charter Implementation Act - Personal Information & Data Protection Tribunal Act
- Privacy and Data Protection, 2021
- Draft Data Privacy Bill, 2020

Moreover, in a data economy proliferated by cloud computing and remote working due to the COVID-19 pandemic, data privacy or data protection has emerged as a strategic business imperative, and not an IT task or a mere compliance check anymore.

According to a study by CISCO, investing in data privacy provides businesses with benefits beyond regulatory compliance[7], such as

- Helped minimize the delay in sales due to privacy issues (3.4 weeks after investment in privacy vs 5.4 weeks without)
- Helped reduce the probability of a data breach (74% after investment in privacy vs 89% without)

Solutioning Privacy Engineering

An effective privacy engineering strategy is inevitable for a forward-looking privacy program – the main focuses must be culture, people, processes, and technology. Privacy needs to be instilled as a 'culture' so that a shared vision of appropriate use of data is inspired across the organization. Relying on 'people' alone is not sufficient – they must be empowered by leveraging 'technology' and implementing the right 'processes' to achieve the privacy objectives.

Therefore, to become a secure and compliant system, data privacy principles need to be incorporated throughout the system development lifecycle. Furthermore, it must be 'by default' and 'by design' instead of retrospective additions or an afterthought. This means privacy must be a core feature on the product roadmap from the onset, i.e., during the ideation phase, or preparing product development notes.

There is no specific set of activities that organizations must perform to incorporate privacy by design; it's more of risk profiling, anticipating the incidents and ensuring that appropriate technical as well as organizational measures are implemented to tackle them. Following are some of the key principles:

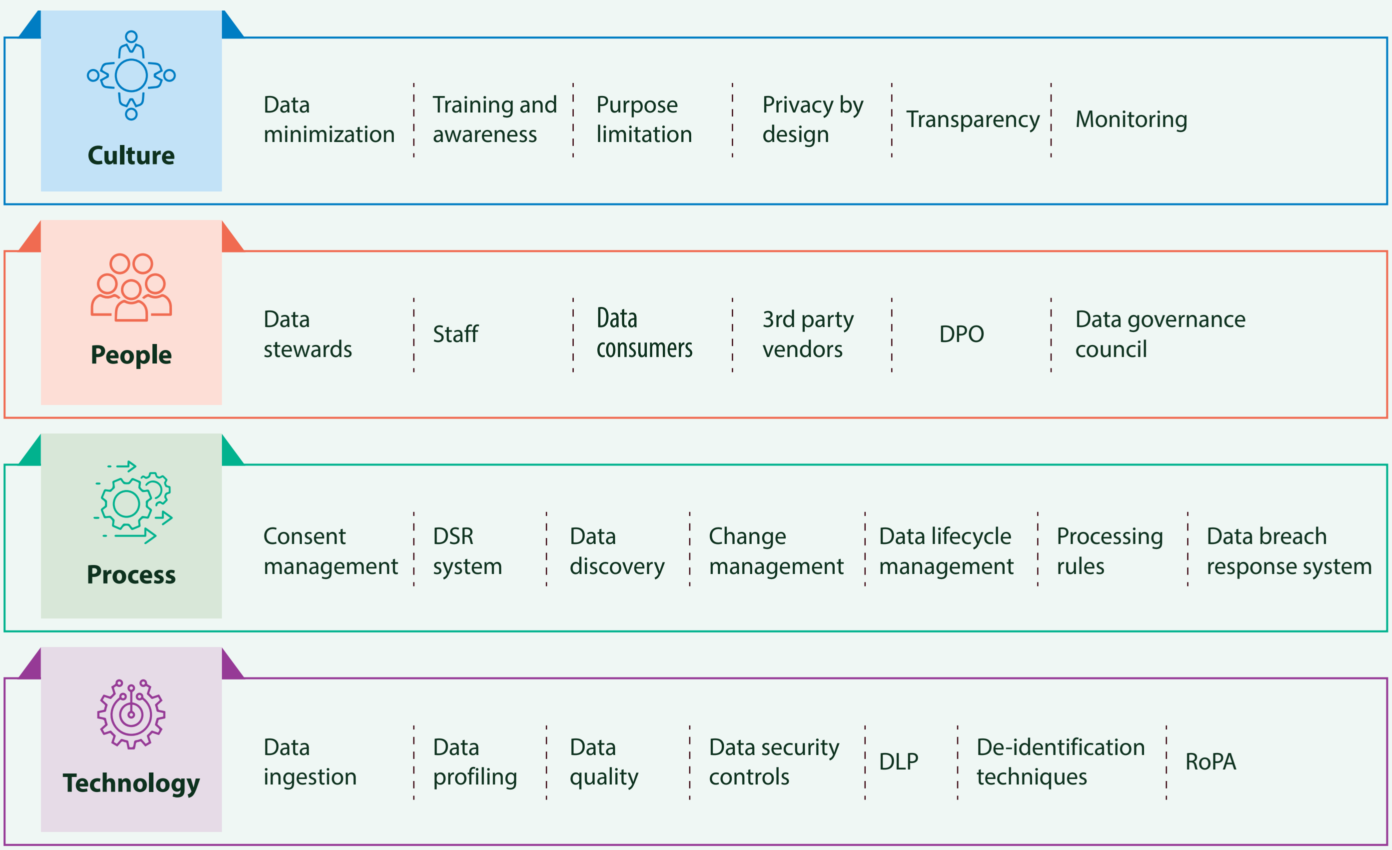
- Data minimization: This principle offers the most straightforward way to reduce the privacy risks, besides providing a sustainable approach to address the 'big data problem'. Organizations must assess the amount of data that they need for their business activity as well as the extent of processing of the data being collected. This will help limit the volume of data to what is absolutely necessary. Furthermore, once the lawful purpose of holding the data ceases to apply, it must be deleted immediately.
- Purpose limitation: It must be ensured that the data is handled only for the purpose it was originally collected for. This means that the reason for processing must be presented to the user in clear terms and they must be given complete control over their data on how their data is being used. To ensure this, a strong data traceability mechanism and Record of Processing activities (ROPA) must be put in place.
- Data security controls: Strong security control measures must be implemented to limit both physical as well as digital access to data regardless of state (at rest or in transit). Its goal is to maintain confidentiality, integrity, and availability of data. This includes features such as Access Management, Encryption, Data de-identification mechanism, Data Loss Prevention (DLP) etc.
- Staff awareness: Most often, cyber-attackers ensure that one individual

falls for the attack, putting the entire organization at risk, as it's easier to trick an individual than penetrate the organizations' network. Organizations must create and promote a culture that perceives security and privacy as a collective responsibility rather than an IT department's chore. Therefore, employees must be made aware of the value of the information they possess and the responsibility that it entails upon them. This can only be achieved by investing in continuous training and staff awareness programs to combat the evolving and sophisticated techniques employed by the attackers.

- Transparency: Organizations must provide information about what and how the data subjects' data is being processed and what their rights are. This is needed so that they are assured of confidentiality and can exercise their rights and make more informed decisions. The information being shared with them must be easy to understand.
- Third-party compliance: Organizations must implement robust audit mechanisms and conduct due diligence to secure compliance assurance from third-party processors or outsourcers. According to a study by eSentire, 44% of firms suffer a data breach due to third-party vendors.[8]
- Default privacy settings: It must be ensured that all systems are configured with default settings that are as privacy-protective as possible. Features include automatic timed logouts, providing users with sufficient controls etc.
- Data audit: Organizations must maintain audit information and document what data they hold, what it is processed for and their data protection implementation. This is needed to not only drive the privacy program, but also demonstrate compliance, when required. Also, a regular review of all the 'processing' activities is required which must be documented.

In practice, a robust privacy engineering mechanism needs to be in place for each phase of the product development lifecycle, such as requirements scoping, solution design, build, testing and go-live.

Figure 4: Data Privacy Framework



DPO – Data Protection Office, DSR – Data Subjects Rights, ROPA – Record of Processing Activities

First-mover advantages of Data Privacy

On the face of it, proactive and comprehensive implementation of data privacy, particularly in countries where a sovereign data protection regulation is not enforced yet, may seem a daunting and expensive task. However, the benefits and opportunities outweigh the burden. There is a strong need to balance between realizing the business needs and respecting the privacy rights of individuals. Following are some of the key business benefits:

Increased Consumer Confidence

Consumers in the digital age are becoming increasingly conscious and concerned about the use of their personal data.[9] As per a study conducted by Consumers International and the Internet Society, 69% of consumers are wary of mobile applications collecting their personal data . Therefore, focusing on data privacy helps build relationships with customers, which will not only help the brand image and boost the organizations' credibility, but also help better understand the customer's preferences as an opt-in/out or a consent indicates a conscious participation. Maintaining transparency with customers by letting them know how their data is used and appreciating their privacy rights will improve customer confidence and increase customer retention. According to research by Capgemini, 81% of organizations reported a positive impact to their brand image post-implementation of GDPR.[10]

Becoming Future Proof

In a globalized world, preparing for a data privacy initiative makes organizations compliance-ready and gives them an edge over their competitors. They would have already completed the foundational work necessary to comply with the inevitable data protection regulation. This will help organizations position themselves as an innovator and global leader in data governance, given the fact that such laws will eventually emerge in all major countries across the globe.

Improved Data Management

With a fostering data economy in today's digital age, data management holds significance more than ever. It is considered a key element in business operations and drives an organization's success. A comprehensive data strategy can't be crafted without incorporating the principles of data privacy. Principles such as data minimization, data profiling, data quality checks and audit frameworks would enable businesses to leverage their data potential, resulting in more refined data management processes.

Reduced Risks

No organization can afford to take the risk of a cyber threat or a data breach; given the impact it can have on the brand image as well as the financial implications. The recent Cambridge Analytica data breach[11] is a textbook example of how privacy can impact the integrity and reputation of an organization. By being proactive, organizations would be able to focus on security and privacy aspects and plan for remediation strategies, since they would now know where the sensitive data is being stored in their systems, thereby minimizing the risk of data breaches.

Reduced Costs

Becoming privacy-ready helps organizations cut costs, as against the general perception that it's a financial burden. By following the data protection principles, organizations would:

- Save on the storage and processing costs by getting rid of redundant and obsolete data.
- Reduce the data maintenance expenses.
- Avoid the retrofit costs when the regulation finally arrives.
- Be left with high-quality data, which means more reliable decision-making.

Proactive Implementation Methodology – Transition Ready

Global applications, though driven by region specific data protection laws, need to have uniformity in terms of the idea of data protection.

Consider the following example:

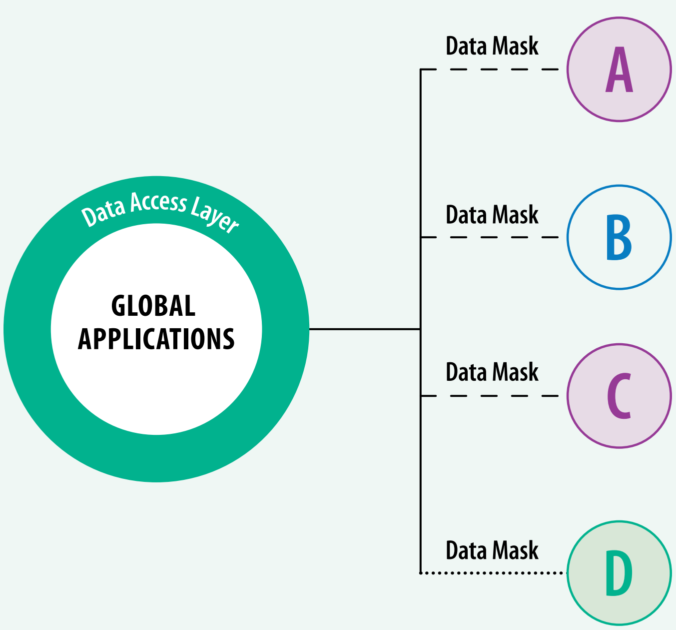
- Region-A and Region-C have similar data protection laws with Region-B having less restrictive laws and Region-D having no data protection law.
- An overarching and proactive data privacy implementation would ensure that Region-D is protected against data breaches as well as it is close to compliance ready when the legislation eventually arrives.
- Though Region-B has a less restrictive data protection law, its data still has an advanced protective layer in Regions-A, C and D.
- Hence, designing the global application in this manner would facilitate a smoother transition with the changing data protection landscape. (Refer to table in next page)

	Data Attribute	A	B	C	D
BEFORE	**Name = "John Smith"**	Considers 'Name' as PII	Doesn't consider 'Name' as PII	Considers 'Name' as PII	No Privacy Law
AFTER	**Name = "John Smith"**	Considers 'Name' as PII	Doesn't consider 'Name' as PII	Considers 'Name' as PII	No Privacy Law. However, Proactive implementation of Data Privacy

Regions A & C consider 'Name' as PII data whereas Region-B doesn't consider it as PII and Region-D doesn't have a data protection law yet. What happens when Region-D implements data privacy? This has been depicted below as a Before vs After implementation of data privacy:

BEFORE						AFTER					
		Can the region access the data?						**Can the region access the data?**			
	Region	**A**	**B**	**C**	**D**		**Region**	**A**	**B**	**C**	**D**
Owner of Data	**A**	XXXX	XXXX	XXXX	XXXX	Owner of Data	**A**	XXXX	XXXX	XXXX	XXXX
	B	XXXX	John Smith	XXXX	**John Smith**		**B**	XXXX	John Smith	XXXX	**XXXX**
	C	XXXX	XXXX	XXXX	XXXX		**C**	XXXX	XXXX	XXXX	XXXX
	D	XXXX	John Smith	XXXX	**John Smith**		**D**	XXXX	John Smith	XXXX	**XXXX**

Figure 5: Globalized Applications – Data Privacy of Region Data – Methodology



PII Data for Region-A
- Region-A Specific Mask.
- Considers 'Name' as PII Data

PII Data for Region-B
- Region-B Specific Mask
- Doesn't consider 'Name' as PII Data

PII Data for Region-C
- Region-C Specific Mask
- Considers 'Name' as PII Data

Region-D
- Region-D has No Data Protection Laws.
- 'Name' is protected in the region because of proactive implementation.

Conclusion

It is only a matter of time before more countries across the globe enforce a sovereign data protection law. It, therefore, becomes pertinent to contemplate about implementing data privacy forthwith, which will help place your organization ahead of the curve.

Furthermore, customers must be viewed as 'allies' and protecting their privacy rights will not only boost brand loyalty, but also manifests as a business enabler, not a showstopper.

References:

1. https://www.statista.com/statistics/871513/worldwide-data-created/
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. https://www.forbes.com/sites/waynerash/2022/02/25/cisa-issues-shields-up-warning-about-russian-cyber-attacks/?sh=48de9d9d3748
4. https://www.weforum.org/agenda/2019/01/biggest-global-risks-facing-our-world/
5. https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html
6. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
7. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf
8. https://www.esentire.com/blog/nearly-half-of-firms-suffer-data-breach-at-hands-of-vendors
9. https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/
10. https://www.capgemini.com/gb-en/wp-content/uploads/sites/3/2019/09/Report-%E2%80%93-GDPR.pdf
11. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

Authors

Mohammed Arifuddin works as a Data Privacy Architect with Data & Analytics unit at Infosys. He has 13 years of experience in driving implementation of strategic initiatives in Data management and building Data privacy solutions. He has extensive knowledge in GDPR, holds a PG certificate in Cyber Law and is a OneTrust Certified Privacy Professional.

Prashanth Kumar M S is a Senior Technology Architect with Finance unit at Infosys. He has 19 years of experience across different clients to design and deliver key projects in Data Sourcing. He has worked on implementing Data Security Layer across regions for a leading investment bank and making applications GDPR compliant.