LTIMindtree

Whitepaper

Data Privacy as a Strategic Business Enabler GDPR under the Lens

by Ritu Khanna

Table of Contents

Abstract

GDPR came into effect on May 25, 2018, becoming the most visible data regulation in the world. Not only has it given residents of the European Union new rights regarding the use of their personal data, the GDPR has also provided organizations a single consistent data management standard to meet. This has set a path for legislations across the world to follow.

Since GDPR came into effect from 2018, much has changed in the last three and a half years. 2020 and beyond has accelerated digital transformation, and subsequently cyber risks. Data proliferation, voluminous transitions to cloud, and accessibility has put new challenges and questions to the CISO, CDO and CTO.

The regulator is not left far behind in this journey. What started initially as a pause in privacy monitoring during the early Covid lockdowns, emerged as increasingly relevant, and of importance for the regulator to continue its checks and balances across regions and industries as organizations needed to increase data tracking, health, and productivity analysis and convenience services to employees and customers alike.

Privacy At-A-Glance

How is privacy maturing as a concept?

Back to the early years of the 21st century, we were universally engaged in social networks and online safety, security awareness had become widespread. The websites or channels utilizing Secure Socket Layer (SSL) were becoming more pervasive. Simultaneously, the appearance of the privacy policy and terms of utilization were becoming standardized. Perpetually, both were written in such thick lawful language that only a few of us could understand how our data was being shared or utilized. We tapped on the "accept" box and generally became part of an option that could be greater than ourselves. With the growth of online platforms, organizations started capturing the customers' data and some would protect this data whereas some would not.[1]

Three years ago, privacy was only about meeting certain set of regulatory guidelines. Today, it is a complete alignment of privacy, security, and governance. So, there is a transition from merely meeting the regulatory standards to a strong legal framework with detailed guidelines.

Data privacy risks that have surfaced in the recent past

Businesses face various data privacy risks when they collect, process, and store personal data or Personally Identifiable Information (PII). IDC predicts that the collective sum of the world's data will grow from 33 zettabytes this year to a 175 zettabytes by 2025, for a CAGR of 61 percent. Some of the most common risks are listed below.

- **Risk of holding too much personal data –** Most organizations require additional data for analytical purposes or to monetize on the collected data. It's important to understand all aspects of data processing before storing and collecting any additional data, which differs from the current business purpose or lawful basis of processing. Data controllers are trying to get a better understanding of the PII risk they carry by bringing increased visibility to the personal data, what data is collected, where is it stored, who is it shared with, and what security policies are applied to the data.
- **Lack of transparency with respect to collection of data and its use** – Data privacy regulations like GDPR often require a clear explanation of what personal data is collected and used. This information needs to be publicly available and usually resides in policy documents such as a privacy policy, cookie policy, and terms of use statement. GDPR has requirements that companies must divulge all the personal data stored about a person if that person requests that information. Failure to respond to information requests will cause the organization to fall out of compliance with the regulation. Most organizations fail to streamline response processes around data transparency and are not able to engage their employees and customers in a participative manner on their own data. Not having sufficient consent management process in the organization is a classic example.
- **Insufficient data security –** Applications, including web applications, on-premises applications, and legacy applications exposed to the web through modern APIs, storing personal data should be secured. If not secured, the personal data is at risk to be stolen or breached.[2] If nothing else, the last one year has taught us that the future is fraught with cyber risks, data breaches, and data loss. Organizations are immediately stepping up their defense and coping mechanisms through multi-layered data security. New and flexible technology solutions are constantly being innovated using encryption, masking, tokenization, hashing, etc.

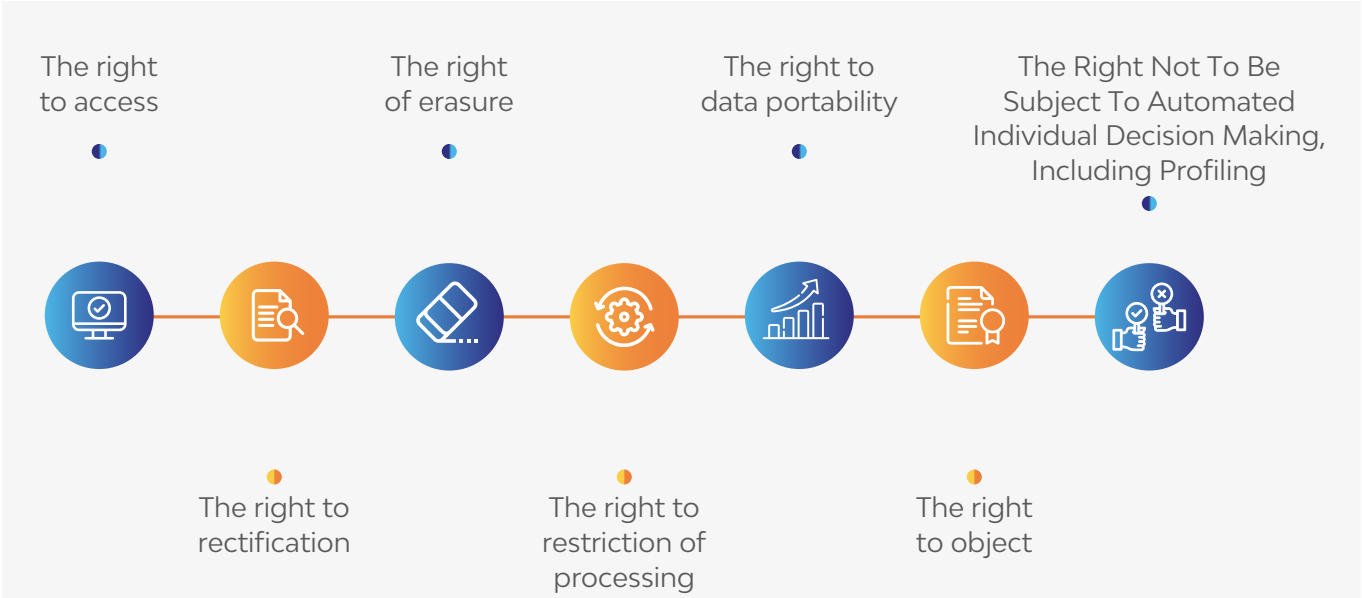
It is now well known that regulators are imposing hefty fines for GDPR violations, and that globally regulators are following suit to keep large data aggregators in check. Apart from keeping their own process in check, organizations must also reassess their supplier selection processes and existing supplier agreements to ensure compliance with the GDPR. Non-inclusion of privacy and protection terms increases the risk of non-compliance.

To address this requirement, specialized privacy preserving technology products have emerged and are constantly solving for the dynamic privacy risk landscape. They offer data privacy solutions on personal data discovery, classification, data governance, and data security to the organizations to enable compliance with global regulations.

Two trends are emerging to solve for the privacy continuum. On one end, there are products solving for varied use cases of privacy. Point solutions that are addressing one or few capabilities at a time across privacy, governance, and security required on data. On the end of the continuum, there are advisory and industry groups researching and recommending frameworks for applying successful privacy technology.

There is a middle territory that belongs to the service providers invested in the privacy domain, have products and talent that ensure long term sustainability of privacy solutions and successful implementation of privacy technology. Few IT service organizations have the ability today to holistically solve for privacy, governance, and data security.

Global Response to the Privacy Imperative



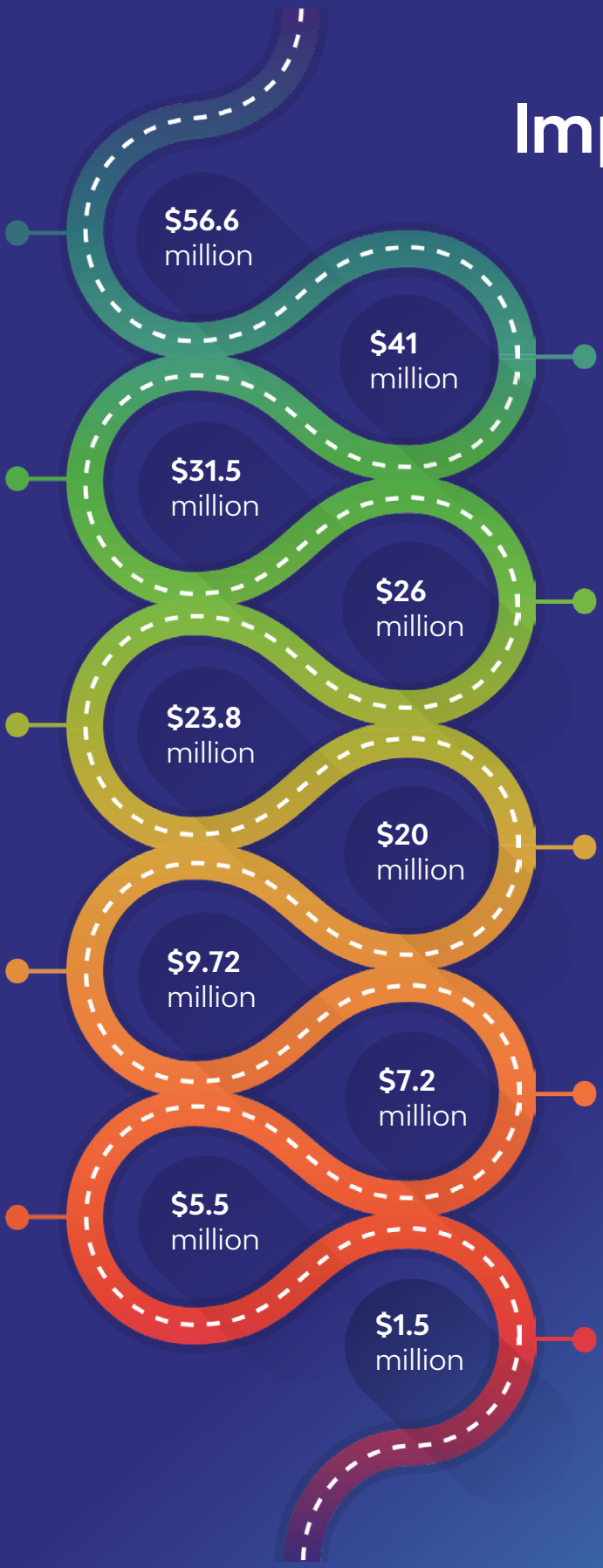
GDPR has inspired new privacy laws around the world and has focused global attention on privacy with the United Nations reporting about 66% of countries currently have data protection and privacy legislation.[4] According to Gartner, by 2023, 65% of the world's population will be covered by modern data privacy laws which means companies that process or collect data will have to coordinate and comply with multiple regulatory frameworks with a high cost for non-compliance.[7]

According to a report by DLA Piper, between January 2020 and January 2021, data breach notifications under GDPR rose 19%, while fines increased by 40%. This double-digit growth is expected to continue in the foreseeable future considering evolving regulations worldwide and increasing consumer awareness of their rights.[6]

According to research from DLA Piper, between January 26, 2020, and January 27, 2021:

- GDPR fines rose by nearly 40%
- Penalties under the GDPR totaled USD 191.5 million
- Data protection authorities recorded 121,165 data breach notifications (19% more than the previous 12-month period)

Fines Imposed



American multinational technology company — $56.6 million

$41 million — Second largest GDPR fine – German clothing retailer

Italian telecommunications operator — $31.5 million

$26 million — Flag carrier airline of UK

American hotel chain — $23.8 million

$20 million — European telecom company

British multinational telecom company — $9.72 million

$7.2 million — Spanish multinational financial services company

Italian telecommunications company — $5.5 million

$1.5 million — German health insurer

2020
2021

A quick view on other regulations

2019 and 2020 brought several major developments in the world of data protection legislation. More than 60 jurisdictions around the world have proposed postmodern privacy and data protection laws, following the introduction of the GDPR in 2018. Some of the notable regulations are mentioned below:

CCPA – The California Consumer Privacy Act directs businesses in their digital collection, storage, and security of information of California-based customers. California Privacy Rights and Enforcement Act (CPRA) amends various parts of the existing CCPA with additional security.

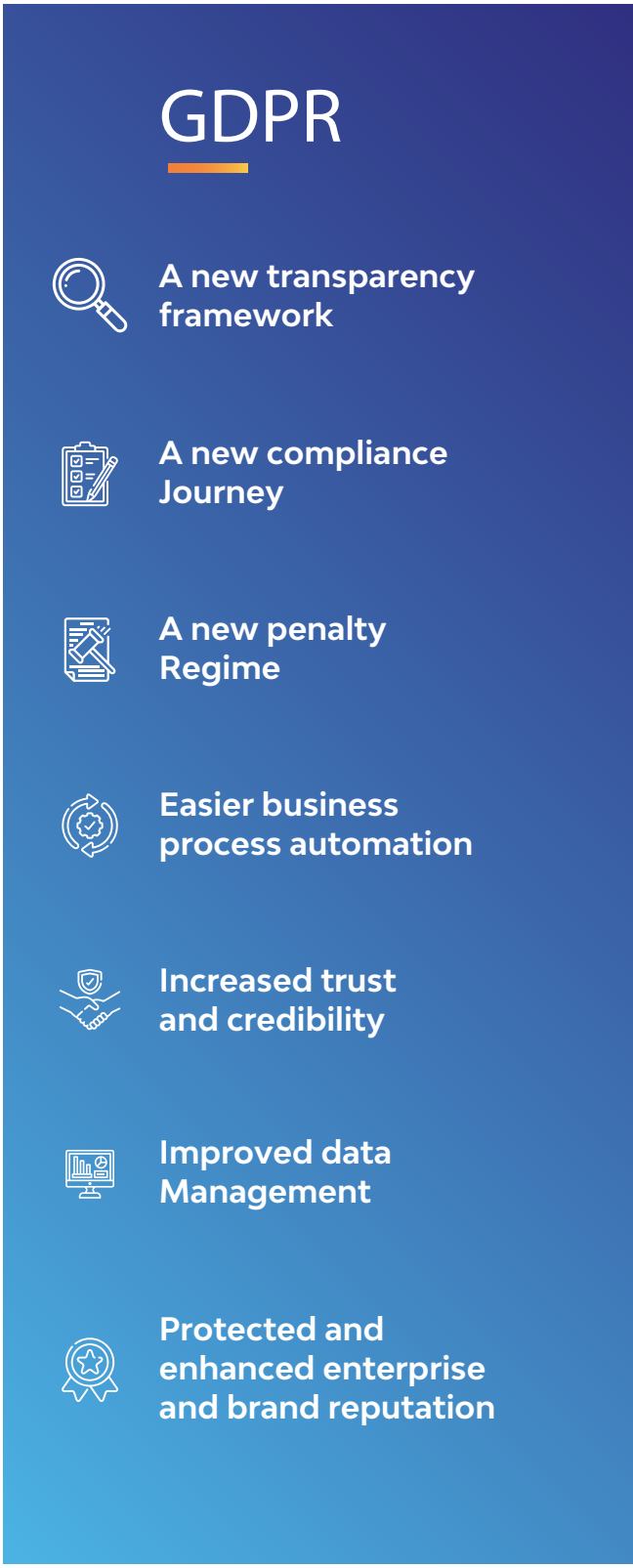
PIPEDA - Canada's federal data protection law, the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to organizations operating in the private sector and regulates how businesses collect, use, and disclose personal and sensitive information.

POPIA - The purpose of South Africa's Protection of Personal Information Act (POPIA) is to protect people from harm by safeguarding their personal information, to prevent their money and identity from being stolen.

PDPA – Singapore's PDPA recognizes both - the rights of individuals to protect their personal data, and the needs of organizations to collect, use, or disclose personal data for legitimate and reasonable purposes.[8]

PDPB - India's Personal Data Protection Bill (PDPB) is currently in draft form and looks set to be one of the strictest and most comprehensive data privacy laws in the world. It will impose obligations on practically all businesses operating in India.

While each legislation will have its own interpretation of consumer rights on privacy and its own empowerment of the regulator, what is undeniable is that Privacy is a lasting socio-economic- political issue that will require the governments and the industry to work together to solve.



Data Protection in the New Normal

In March 2020, after Covid-19 hit countries all over the world most companies shifted to remote working model overnight. But as the pandemic entered its second year, leaders have been surprised to learn that people can work just as productively from home. Businesses in many sectors are beginning to recover from the pandemic, and many are likely to look for a fast and efficient way to bounce back to their usual operations and revenues. Business pundits and analysts alike are rigorously trying to make sense of the new normal and its implications on privacy. Here are some of the trends leading privacy and data governance to becoming strategic assets to business as the world navigates through new ways of working:

Permanently hybrid ways of working are being designed. According to Gartner, roughly two-thirds of companies are saying they will be moving a portion of their workforce permanently to a remote work model. Cybersecurity is no longer a hygiene factor and business can no longer rely on physical boundaries and traditional perimeters to guard the company assets. All further growth of businesses will need to start with putting a cybersecurity and privacy strategy in place, rather than building it in as an afterthought.

Remote working has also exploded the opportunity to offshore erstwhile restricted business operations. With a proven remote working model, most companies are looking at increasing offshoring to be able to reduce operational disruptions and costs during and after the pandemic. Offshoring is even more attractive to companies because of the benefits it can bring to their business in the long run such as increased productivity, business development and expansion, etc. Processing data across regulatory boundaries, sharing of privacy responsibilities, and liabilities will make for some interesting remodeling of business processes.

Over two billion people worldwide purchased goods or services online last year. **The phenomenal increase in online transactions has pushed the digital agenda across industries.** Subsequently, the attack surface, threat actors, and risk impact have all compounded. There needs to be a well thought through strategy for privacy covering breath of services and depth of customer data for every corporate and government entity. The question no longer is about will we be subject to a cyber-attack. The question is more about how we can minimize the impact of cyber-attack on our organization.

Transition to cloud has by far been the most significant change to be felt in technology modernization. Does the cloud technology today have sufficient data security controls? Does the presence on cloud absolve the organization of its responsibility to protect consumer privacy? How will the segregation of duties between cloud provider and cloud consumer ultimately pan out in the eyes of the regulator and the end consumer at large?

Technology is increasingly getting productized. It is also becoming specialized to cater to **industry-specific use cases** and dynamics. Similarly, interpretation of consumer privacy and the tradeoff between sharing information and service convenience needs to be carefully studies in context of industry. For example, while the consumer may be sensitive about sharing their location and behavioral information with media companies, the consumer may use fitness trackers or smart watches that give them insights based on their behavior.

As the operational demands of privacy programs increase, it is becoming clear that the leaders will set themselves apart by setting up **metrics and benchmarks** while investing in privacy technology. It is no longer enough to focus on the risk metric and simply making sure the organization isn't breaking the law. For example, the data may show that a certain department is the source of a significant number of privacy incidents, or you may see a department with fewer than average incidents. Effective training and day-to-day metrics can lower the risk of incidents in the first scenario, and ensure incidents are accurately discovered and reported in the second.

By far **GDPR has emerged as the gold standard as far as privacy goes.** Having already influenced major global regulations like the US, Brazil, India, UAE, Singapore, and Japan since it came into force, the GDPR continues to be the influencing force behind global privacy regulations being published/coming into effect. As Data Protection Authorities across each Member State in the EU gain more effective teams, implementation of the GDPR will likely increase and become more enlightened. For example, recently the Commission Nationale de l'informatique et des Libertés (CNIL), the French Data Protection Authority, announced that it will begin conducting audits of websites to determine if a website complies with the CNIL's guidance on web cookies. It remains to be seen if similar gold standards can be achieved in the control implementation framework.

Privacy preserving technology solutions continue to evolve to assist with not only readiness efforts, but also to automate portions of privacy management program once it's established. This is particularly important for the handling of subject rights requests and the processes for Consent & Preference Management (CPM). By year-end 2022, more than 1 million organizations will have appointed a privacy officer (or data protection officer). Increased regulation will lead organizations to hire capable, empowered senior-level privacy officers to deliver both compliance and customer satisfaction.

Considering the wide-ranging nature of the GDPR, execution, and deployment challenges were inevitable and were to be expected. Organizations and regulators appear to be learning over time, gradually improving data protection practices, serving to reduce breaches and enhance the privacy of individuals. However, arguably the GDPR's biggest legacy to date has been to grow awareness of privacy issues and rights amongst the general population, which is vital in an increasingly digitalized world, where criminal uses of data and cybercrime are growing risks.

Use Case: Privacy Impact in Insurance Industry

Personal data at the heart of the business

The insurance industry handles personal data daily; this includes both high-risk data (bank details, social security number, details of offences and court rulings, and real-time global positioning data) as well as sensitive data (health, biometric data, etc.). Due to this, the insurance industry is in the front line as far as the protection of personal data is concerned.

GDPR is a game changer for companies that have taken a datacentric privacy first approach to make efficient business decisions. Improved operational efficacy, greater credibility with customers and employees, a reduced threat landscape, and enhanced brand value are benefits to be derived across customer touchpoints of underwriting claims. Another area in which insurers score big is in cyber risk insurance. With the scale of fines under GDPR, the costs resulting from a cyber-attack can no longer be seen as an acceptable cost of running a business. More and more companies will look to risk-insure their businesses against cyber-attacks.

In the pre-GDPR EU, breaches often went under the radar as there were no regulatory requirements for companies to report breaches. After the implementation of GDPR, this has changed due to requirements for mandatory breach notifications to regulators and in some cases data subjects (Art. 33, 34). This will likely result in a surge in demand for cyber insurance products and services to avoid, mitigate, or transfer the risk of cyber perpetrated breaches. With only a small number of insurers offering cyber insurance today, there is a tremendous opportunity for others to establish a footing in this growing market and develop all-encompassing cyber insurance products.

The intent should be to provide end-to-end cyber risk management solutions covering cyber threat intelligence, expert consultation, legal and forensics assistance, as well as adequate cyber indemnity from first-party costs and third-party claims arising from a data breach. It will be a win-win situation if insurers, by way of their holistic cyber risk management offerings, are able to help their clients alleviate their cyber risk profiles. Now, it will be interesting to know whether insurers will match their cyber insurance cover to the colossal EUR 20 million (or 4% of global annual turnover, whichever is higher) fines entailed by GDPR. Equally fascinating will be the final position regulatory authorities take on whether cyber insurance can legally indemnify the full penalty under this European data privacy regulation.

GDPR and Cyber insurance

Cyber insurance generally covers losses arising from the disclosure of personal information in a data breach or cyber incident. The GDPR, however, regulates the processing of personal data. As a matter of public policy, regulatory fines are uninsurable in some EU Member States.[9]

Many policies include coverage for regulatory fines, as those fines are "recoverable at law". This is where the difficulties lie. After all, fines are meant to be a deterrent, and if businesses can make an insurance claim to avoid paying up, this deterrent effect is lost.

Lawmakers recognize this, which is why there is a long-established "illegality defence" that prevents companies and individuals from using insurance to avoid the consequences of their illegal actions. Yet, there hasn't been a case before the UK courts to decide on whether a data regulator fine can be lawfully covered by insurance. But we already know from other areas of law that fines of a "penal" nature (i.e., designed to punish the wrongdoer) are not recoverable.[10]

Conclusion

GDPR has been one of the significant factors governing digital business rules in the recent times. It has set the building blocks for a data privacy and protection landscape that is consumer centric. As more and more nations adopt similar privacy governance frameworks and evolve regulations around it, new ways of conducting business are surely taking cognizance of engaging privacy strategy and solutions. This is hand in hand with security solutions enabling access to business and data from anywhere. As data privacy and data protection continues to sweep the globe this is not a movement to be overlooked. Now is the time for organizations to put a greater emphasis on their practices and make privacy more than just an agenda of corporate compliance.

1. https://www.alleywatch.com/2018/05/the-state-of-data-privacy-then-and-now/
2. Why Data Privacy Matters & How to Build a Privacy Compliance Program (hyperproof.io)
3. https://www.snowflake.com/trending/data-platforms
4. Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance by Graham Greenleaf :: SSRN
5. GDPR at Three (iapp.org)
6. DLA Piper GDPR fines and data breach survey: January 2021 | Insights | DLA Piper Global Law Firm
7. Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations
8. https://www.endpointprotector.com/blog/10-data-protection-regulations-you-need-to-know-about/
9. https://www.jonesday.com/en/insights/2018/11/gdprs-potential-fines-and-other-exposures-raise-cy
10. https://www.privacycompliancehub.com/gdpr-resources/can-cyber-insurance-protect-my-organisation-from-the-gdpr/

Author Profile

Ritu Khanna
Data Privacy Practice Head, LTIMindtree

Ritu leads the Data Privacy practice at LTIMindtree, working with clients to adopt "privacy by design" in their data management and governance operations. Ritu's global experience spans across consulting, technology, and operations across BFSI, Fintech, Consumer, and Lifesciences.