# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

# DISCLAIMER

ISSN: 2582-6433

# EDITORIALTEAM

## EDITORS

### Dr. Samrat Datta

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*

### *Dr. Namita Jain*

*Head & Associate Professor*
*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*

*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

**ISSN: 2582-6433**

## Mrs.S.Kalpana

Assistant professor of Law

*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*

## Avinash Kumar

*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

ISSN: 2582-6433

# ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

# THE IMPACT OF GDPR AND OTHER REGULATIONS IN COMMERCIAL LAW AND DATA PRIVACY

AUTHORED BY - AKSHAYA R & KISHORE CHANDURU
ASSISTANT PROFESSOR
VISTAS, CHENNAI

## Introduction

Personal data has grown to be a valuable asset in the digital age, propelling economic growth and commercial strategy. However, serious questions concerning consumer rights, security, and privacy have been brought up by the growing amount of personal data being collected, processed, and transferred. Governments all over the world have implemented strict data protection rules to address these problems, with the European Union's General Data Protection Regulation (GDPR) being the most significant framework. In addition to redefining data privacy rights, GDPR has established a global standard that has influenced other laws of a similar nature, including the Digital Personal Data Protection Act (DPDP) of India, the California Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL). Commercial law has been significantly impacted by the execution of these standards, which have an effect on contractual agreements, digital marketing, corporate operations, and cross-border data transfers. Businesses must now embrace privacy-by-design principles, employ strong data protection procedures, and make sure they are in conformity with changing legislative requirements. Data protection is a major concern for companies all over the world since non-compliance can result in significant fines, harm to one's brand, and legal ramifications. The effect of the GDPR and other data privacy laws on business law is examined in this study. It looks at the main obstacles that companies must overcome to comply, how GDPR is influencing international data privacy regulations, and the legal ramifications of data breaches. The article also examines the ways in which privacy rules affect business dealings, such as data processing agreements, e-commerce, and digital marketing. Businesses may reduce risks, handle the intricacies of data privacy rules, and gain the trust of customers by being aware of these legal frameworks. The purpose of this study is to offer insightful information about how data protection is changing and how it affects commercial law in the global economy.

ISSN: 2582-6433

## GDPR and Other Data Privacy Laws: A Comparative Study

A global standard for data privacy regulations was established in 2018 with the implementation of the General Data Protection Regulation (GDPR) by the European Union. Its impact is not limited to Europe; it has influenced similar laws all around the world. The GDPR is compared to other important data privacy laws, including the Digital Personal Data Protection Act (DPDP) of India, the California Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL).

With a focus on values like accountability, transparency, equity, and lawfulness, GDPR offers a thorough framework for data protection. It gives data subjects rights such data portability, erasure (the right to be forgotten), rectification, and access. Serious fines of up to €20 million or 4% of a company's worldwide income are imposed for noncompliance.

The CCPA, on the other hand, which went into force in 2020, prioritizes consumer rights over broad data protection. It gives Californians the ability to opt out of data sales, to know what personal information companies gather about them, and to have their personal information deleted. Although it is comparable to GDPR, it does not provide for automatic consent procedures or data portability. China's PIPL, which went into effect in 2021, is quite similar to GDPR but has more stringent government regulation. It requires authorization for cross-border data transfers, express agreement for data processing, and more severe sanctions for noncompliance. The law gives authorities broad control over data flow and places a high priority on national security. A consent-based framework is introduced by India's DPDP Act, which was passed in 2023, but it has less compliance requirements than the GDPR. It guarantees user rights including data correction and grievance redressal while streamlining responsibilities for startups and small enterprises. It permits extensive exclusions for government data processing, in contrast to GDPR. The consumer-centric paradigm of the GDPR, the business-regulated openness of the CCPA, the government-supervised restrictions of the PIPL, and the balanced compliance of the DPDP are all examples of regulations that represent regional objectives. Companies that operate globally need to manage these variations to guarantee that data is handled legally in all regions.

## Businesses Face Difficulties in Complying with GDPR

Businesses have many obstacles in ensuring GDPR compliance, especially international firms that handle enormous volumes of personal data. Rethinking data collection, processing, and

ISSN: 2582-6433

storage while striking a balance between operational effectiveness and legal requirements is necessary for compliance. Inventory management and data mapping are two of the main obstacles. Businesses must keep thorough records of all their data processing operations, including what information they gather, how they store it, and if they share it with outside parties. Non-compliance may result from inaccurate record-keeping. Getting and handling consent is another difficulty. Pre-checked boxes and implied consent are insufficient under GDPR, which requires explicit, affirmative user consent for data collection. To ensure compliance and reduce user friction, businesses must put strong procedures in place for obtaining, documenting, and managing user permissions. The problem of cross-border data exchanges is complicated. Due to the EU-US Privacy Shield agreement's invalidation, companies are now forced to rely on Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). However, compliance is challenging due to regulatory ambiguity, especially for multinational corporations. In some circumstances, GDPR also mandates that businesses designate Data Protection Officers (DPOs), which raises operating expenses. Businesses must also adhere to privacy-by-design guidelines, which guarantee that data security features are included into goods and services from the very beginning. Heavy fines, harm to one's reputation, and legal ramifications can result from noncompliance. For instance, Amazon was fined €746 million for violating the GDPR in 2021. To satisfy regulatory requirements, companies must thus invest in secure data management systems, train staff, and update their compliance policies on a regular basis.

## The GDPR's Influence on International Data Privacy Guidelines

The GDPR has had a major impact on data protection legislation around the world, creating a framework that has been adopted or modified by other governments. It has pushed countries to fortify their data privacy rules by setting a precedent for consumer rights, business accountability, and regulatory enforcement. Countries that have updated or implemented new data protection regulations in line with GDPR principles include Brazil, Japan, South Korea, and Canada. The consent-based model and enforcement procedures of the GDPR are mirrored in the Brazilian General Data Protection Law (LGPD), while the cross-border data transfer criteria of the GDPR are mirrored in Japan's Act on the Protection of Personal Information (APPI).

Global business practices have also been impacted by GDPR. Because of the GDPR's extraterritorial reach, many businesses—including those outside the EU—voluntarily abide by

ISSN: 2582-6433

it. Regardless of where its headquarters are located, a business must abide by GDPR regulations if it handles the data of EU citizens. As a result, multinational corporations have restructured their data privacy policies to ensure uniformity across markets.

Additionally, tech behemoths like Google and Meta have updated their privacy rules in response to GDPR. Additionally, it has sparked legal debates about the creation of ethical AI, guaranteeing that machine learning models adhere to data protection regulations.

Nonetheless, some areas have opposed GDPR-style rules. The US relies on sectoral laws like the CCPA in lieu of a comprehensive federal data privacy law. China's PIPL adopts a more stringent stance, giving state authority over data protection first priority. Notwithstanding these variations, GDPR continues to be the gold standard for worldwide data protection, impacting upcoming legislative changes.

## GDPR and Other Regulations: Data Breach and Liability

Under GDPR and other data privacy laws, data breaches present serious financial and legal consequences. Businesses who don't protect user data risk severe penalties, legal action, and harm to their reputation. According to GDPR, companies must notify authorities of data breaches within 72 hours of becoming aware of them. If a breach poses a high risk to the rights of affected individuals, companies are required to notify them. Fines of up to €20 million or 4% of yearly global turnover may be imposed for noncompliance. For example, Marriott was hit with a €20 million fine for a breach that affected 339 million customers, while British Airways was fined €22 million in 2020 after hackers stole client data. These incidents demonstrate the necessity of strong cybersecurity defenses. Similar criteria are imposed by other regulations. Customers have the right to sue businesses under the CCPA for data breaches, and the statutory damages for each infraction can range from $100 to $750. Authorities can impose harsh punishments, such as suspending commercial activities, under China's PIPL. Businesses must implement multi-factor authentication, robust encryption, and frequent security audits to reduce liability. Investing in cybersecurity safeguards consumer trust and brand reputation in addition to ensuring compliance.

## Data Privacy Regulations and Commercial Law Intersect

Contracts, digital marketing, and e-commerce have all been impacted by data privacy rules, which have revolutionized commercial law. Companies are now required to incorporate GDPR

ISSN: 2582-6433

compliance into their contracts, especially those pertaining to data processing and third-party vendors. Businesses are required by GDPR to make sure data processors follow stringent security guidelines. If this isn't done, there may be joint accountability for data breaches. As a result, contract negotiations are being more closely examined, and businesses are requesting indemnity clauses and compliance assurances from service providers. GDPR has limited cookie-based tracking and targeted advertising in digital marketing. Platforms that depend on ad revenue are impacted since companies must get users' express consent before gathering behavioral data. Similar restrictions are placed on monitoring technologies by the ePrivacy Directive, also known as the "Cookie Law," which compels businesses to use consent-driven approaches. In order to enable clients to move their data between service providers, e-commerce companies must also adjust to data portability rules. Although this has boosted competition and empowered consumers, its execution poses technological difficulties. All things considered, GDPR and other laws have changed how firms conduct business, necessitating the adoption of privacy-focused legal frameworks that strike a balance between profitability and compliance.

## Conclusion

GDPR and other data privacy laws have had a significant impact on commercial law, changing how companies manage personal information. GDPR has established a worldwide norm that has impacted regulations that represent regional interests, such as the CCPA, PIPL, and DPDP. However, complicated requirements like data mapping, consent management, and cross-border data transfers make compliance difficult. Businesses who don't comply risk harsh financial fines, damage to their brand, and legal repercussions. Furthermore, GDPR has been significant in influencing worldwide privacy standards and encouraging companies to implement privacy-focused policies. Because data breaches are still dangerous, cybersecurity and adherence to the law are crucial. Legal and business strategies are further complicated by the requirement that digital marketing, e-commerce operations, and commercial contracts all adhere to strict data protection regulations. Notwithstanding these obstacles, GDPR has improved openness, bolstered consumer rights, and promoted moral data treatment. Some nations balance privacy protection with commercial freedom, while others take a tight legislative approach. To stay in compliance, safeguard client confidence, and stay out of trouble with the law, businesses need to proactively adjust to these changing regulations.

ISSN: 2582-6433

## Suggestion

1. Strengthen Global Compliance Strategies: To reduce compliance risks, companies that operate in several jurisdictions should implement a single data privacy framework that complies with the strictest legal requirements, including GDPR.
2. Strengthen Data Security Measures: To avoid data breaches and lower liability under privacy rules, businesses should make investments in encryption, frequent security audits, and multi-factor authentication.
3. Enhance Consent Management Systems: To ensure compliance with laws like the CCPA and GDPR, organizations should put in place clear, easy-to-use consent procedures that give people control over their data.
4. Create Sturdy Data Processing Agreements (DPAs): To guarantee adherence to data protection regulations and reduce the danger of shared liability, businesses should carefully draft contracts with outside contractors.
5. Track Regulatory Developments: To ensure compliance and business continuity, organizations must keep abreast of new legal requirements as data privacy regulations continue to change and modify their policies accordingly.
6. Invest in Employee Training: To avoid compliance violations and increase internal understanding of privacy responsibilities, organizations should regularly teach staff members on data protection best practices.
7. Adopt Privacy-by-Design Principles: Companies should make sure that privacy protections are ingrained in their operating procedures by including data protection measures into their goods and services from the beginning.

Businesses may manage the intricacies of GDPR and other data privacy regulations by putting these tactics into practice, which will increase customer trust and reduce legal risks.