ILE JUDICIAL AND LEGAL REVIEW

VOLUME 1 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

ILE Judicial and Legal Review

(Free Publication and Open Access Journal)

Journal's Home Page – https://jlr.iledu.in/

Journal's Editorial Page - https://jlr.iledu.in/editorial-board/

Volume 1 and Issue 1 (Access Full Issue on - https://jlr.iledu.in/category/volume-1-and-issue-1-of-2023/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

ILE JUDICIAL AND LEGAL REVIEW

Volume I and Issue I of 2023

ISBN - 978-81-961120-0-4

Published by

Institute of Legal Education

https://iledu.in

PRIVACY AND PERSONAL DATA- "SECURITY HAPPENS TO BE OUR PRIORITY, KNOW WHAT YOU ARE UP TOO"

Author- Rubini B, Student of Sathyabama Institute of Science and Technology.

Best Citation - Rubini B, PRIVACY AND PERSONAL DATA- "SECURITY HAPPENS TO BE OUR PRIORITY, KNOW WHAT YOU ARE UP TOO", *ILE JUDICIAL AND LEGAL REVIEW*, 1 (1) of 2023, Pg. 09-13, ISBN - 978-81-961120-0-4.

ABSTRACT

In our day to day life, our technology evolved more, the usage of internet increased severally over years and our personal data are shared through internet, in media platforms. It is stored in good manner for provide the services for the users; But in some platforms storing personal data are quite dangerous as, there is no much safeguard measures and in some cases, hackers hacking it and misusing it for their profit. According to law taking other's personal data is violating fundamental rights of leyman and Breach of privacy according to article 21 of Indian constitution. Privacy was statutorily recognised globally for the very first time by the UDHR in 1948 through its Article 12[4]. By this paper; we know more about privacy of leyman and personal data issues facing by the users to safeguards the personal data. In this article; we learn more about laws that protecting leyman's privacy and personal data. It suggests some ways to overcome and which support and compromises user privacy while data breach.

Keywords: Data breach, personal data, security, data protection, privacy, GDPR

I.INTRODUCTION:

As we know personal data is information able to identifiable individual or related to identified. An individual can be identified by name or number or by other identifies like email; fingerprints etc. Any information related to specific person is personal information. Personal data that is not identifiable any person is not considering as personal data. Personal data are classified according to their sensitivity; high, medium and low. High sensitivity data are destroyed in an unauthorised transaction like financial records or intellectual property, Medium sensitivity data intended to internal uses like emails, documents. Low sensitivity data are intended to public use like public website content. Personal data misused in number of ways, if it is not maintained secrecy or if respected person doesn't have ability to control their data's. Right to Privacy is also a fundamental right of the people.

Justice K.S Puttaswamy (Retd) and Anr vs Union of India

Right to privacy declared as fundamental right by Supreme Court of India on 24 august 2017. "The right to privacy is inextricably bound up with all exercises of human liberty – both as it is specifically enumerated across Part III, and as it is guaranteed in the residue under Article 21. It is distributed across the various articles in Part III and, mutatis mutandis, takes the form of whichever of their enjoyment its violation curtails".

ILE JUDICIAL AND LEGAL REVIEW

Volume I and Issue I of 2023

ISBN - 978-81-961120-0-4

Published by

Institute of Legal Education

https://iledu.in

II. WHY IT IS IMPORTANT TO PROTECT DATA?

Personal data privacy is important, as more you know about it: it help to protect yourself from huge number of risks. Since, Data protection prevents data information of any person, company, or organization from fraudulent activities, cybercrime, and identity theft. As the protection of the personal data must be higher, is directly proportional to the amount of data stored. Every user must update their protective measures. Data protection follows the principle CIA Triad where C stands for confidentiality, it must be handled only by authorised operators, I stands for Integrity, stored data must be reliable and precise; A stands for availability, data must be safe and reliable available whenever needed. Criminals can use personal data to scam or harass users. Entities may sell personal data to advertisers or other external parties without the user's consent, which may result in the user receiving unwanted marketing or advertisements. When a person's activities are tracked and monitored, it can limit their ability to speak freely, especially under repressive governments.

Lloyd v Google LLC [2021] UKSC 50

Privacy law judgment of the year the UK Supreme Court considered whether a class action for breach of s4 (4) Data Protection Act 1998 ("DPA") could be brought against Google of its obligations as a data controller for its application of the "Safari Workaround". The claim for compensation was made under s.13 DPA 1998. The amount claimed per person advanced in the letter of claim was £750. Collectively, with the number of people impacted by the processing, the potential liability of Google was estimated to exceed £3bn.Lord Leggatt gave the unanimous judgement in favour of the appellant Google LLC.[14]

III. HISTORY OF DATA PROTECTION LAW:

The first data protection law established in Sweden in 1973 came into effect as Sweden's Data Act which passed nearly 50 years ago. Later, Swedish Data Protection authority made illegal for any person or company, organisation whoever has data without license. In late 60s European Union announced their own Data Protection Directive in 1995, it was implemented in 1998, EU were happy as it was followed by all.

In 90's USA approached state to state regulations, but US states doesn't recognize an individual right to privacy, regulations are limited, it is fair if we collected it even without the consent of the user. Later United Kingdom implemented Data Protection Act 1998. As changes occurred: vast increase in technology: private information is uploaded in internet platform.

All from banking to commerce, transport, education to employment evolved over Personal data were shared everywhere through internet. In 2009, EU Commission investigates over public and took public consultation on data protection. By 2012, General Data Protection Regulation were implemented, all new regulations were established in 27 countries (India, Egypt, Australia, China, Brazil, Canada). EU got approval in 2014 and it was adopted by Council of Europe and Europe Parliament in 2016 and it came into effect by 2018. After 20 years enforcement of Data Protection Directive, as whole country must follow regulations implemented.

Warren v DSG Retail Ltd [2021] EWHC 2168 (QB)

Court held that the viability of claims for breach of confidence and misuse of private information against data controllers who have suffered cyber-attacks. In dismissing the claims for breach of confidence and misuse of private information Saini J found that both causes require some form of "positive conduct" by the defendant that is lacking where the cause of the private information being leaked is a cyber-attack.

[14] https://inforrm.org/2021/12/22/top-10-privacy-and-data-protection-cases-of-2021-a-selection-suneet-sharma/

ILE JUDICIAL AND LEGAL REVIEW
Volume I and Issue I of 2023
ISBN - 978-81-961120-0-4
Published by
Institute of Legal Education
https://iledu.in

IV. LEGISLATION THAT GOVERN DATA PRIVACY:

Use and sharing of personal information to 3rd party without consent of user is breach: 137 countries out of 194 countries had legislations to secure the protection of data privacy.

General Data Protection Regulation (GDPR): Specifies how personal data of European Union (EU) data subjects (i.e. individuals) is collected, stored and processed, and gives data subjects the right to control their personal data (including to be forgotten). The GDPR must follow seven key principles for how data controllers and processors should handle personal data: Lawfulness, fairness, and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality (security), Accountability.

National Data Protection Laws: Many countries, such as Canada, Japan, Australia, Singapore, etc., have comprehensive data protection laws in various forms. Some, like Brazil's General Data Protection Act and UK Data Protection Act, are very similar to GDPR. California Consumer Privacy Act (CCPA): Requires consumers to understand what personal data is collected and gives consumers control over their personal data, including the right to tell organizations not to sell their personal data. Children's Online Privacy Protection Act (COPPA) gives parents control over what information websites can collect from their kids.

Health Insurance Portability and Accountability Act (HIPAA) ensures patient confidentiality for all healthcare-related data. Electronic Communications Privacy Act (ECPA) extends government restrictions on wire taps to include transmission of electronic data. Video Privacy Protection Act (VPPA) prevents the wrongful disclosure of an individual's PII stemming from their rental or purchase of audio visual material. Gramm-Leach-Bliley Act (GLBA) mandates how financial institutions must deal with the individual's private information. Fair Credit Reporting Act (FCRA) regulates the collection and use of credit information.[15]

ES v Shillington 2021 ABQB 739

In this case the Alberta Court of the Queen's Bench awarded damages under new "public disclosure of private fact" tort, held judgment for the claimant, Inglis J accepted their submissions that a new "public disclosure of private information" tort should be recognised as a separate cause of action from existing common law statutes.[16]

V. HOW TO PROTECT DATA?

A. Data privacy can be enhanced with the following measures and safeguarded by Choose strong passwords and change them regularly;
B. Use multi-factor authentication (MFA) or biometrics for important accounts; Do not click on links and buttons in emails.
C. Avoid providing unnecessary or unwanted PII; use malicious tools and keep those tools up to date; and use only trusted apps and websites.
D. Data Discovery is 1st step discover which data sets exist in an organization.
E. Data Loss Prevention (DLP) - A set of policies and tools that can be used to protect data against theft, loss or accidental deletion, tools to prevent and recover data loss.
F. Backup – Creates a copy of the data and stores it separately so that the data can be retrieved later if it is lost or changed. Backups are a key strategy for ensuring business continuity when raw data is accidentally or intentionally lost, destroyed, or damaged. Learn more in our data availability guide.
G. Snapshot - A snapshot is similar to a backup, but is a complete image of the protected system, including data and system files. Snapshots can be used to

[15] https://www.cloudflare.com/learning/privacy/what-is-data-privacy/
[16] https://inforrm.org/2021/12/22/top-10-privacy-and-data-protection-cases-of-2021-a-selection-suneet-sharma/

ILE JUDICIAL AND LEGAL REVIEW
Volume I and Issue I of 2023
ISBN - 978-81-961120-0-4
Published by
Institute of Legal Education
https://iledu.in

restore an entire system to a specific point in time.

H. Replication - A technique for continuously replicating data from a protected system to another location. It provides an up-to-date, real-time copy of data, allowing not only recovery but also instant failover to the replica in the event of a primary system failure.
I. Firewall is a utility that allows you to monitor and filter network traffic. You can use a firewall to ensure that only authorized users are allowed to access or transmit data.
J. Authentication and Authorization - Controls that help you validate credentials and ensure user permissions are applied correctly.
K. Encryption – Modification of data content according to an algorithm that can only be reversed with the correct encryption key. Encryption protects your data from unauthorized access even if it is stolen because it cannot be read. Learn more in the data encryption guide.
L. Endpoint Protection - Protects your network's gateways, including gateways, routers, and connected devices. Endpoint protection software often allows you to monitor network perimeters and filter traffic if necessary.
M. Deletion of Data – Limitation of Liability by Deletion of Data No Longer Needed. This can be done after the data has been processed and analysed, or periodically when the data is no longer relevant.
N. Disaster Recovery –The disaster recovery process typically involves setting up a remote disaster recovery site with replicas of the protected systems and switching operations to those systems in the event of a disaster.[17]

VI. RIGHTS OF DATA OWNER:

A. Right to information, when obtaining data, data subjects must be informed about the collection and use of their personal data.
B. The right to access their data, Data subjects may request a copy of their personal data through a data subject request.
C. Data controllers must explain how it is collected, what is processed and with whom it is shared.
D. Right of rectification, the data of the person concerned is inaccurate or incomplete, he has the right to ask you to correct it.
E. Right to erasure, Data subjects have the right to request the erasure of personal data concerning them within 30 days for specified reasons.
F. The right to restrict processing, Data subjects have the right to request that their personal data be restricted or blocked (although you can still store it).
G. Right to data portability, Data subjects can securely transfer data from one electronic system to another at any time without affecting its availability.
H. Right of objection, Data subjects can object to how their information is used for marketing, sales, or non-service related purposes. [18]

VII. CONCLUSION:

Every person are entitled to get right to privacy, basic fundamental right according to Article 21 Right to Privacy is included in right to life in Indian Constitution. It's everyone own duty to keep their personal data with more protection and different variant legislations are framing more according to our technology and breaches. All humans are entitled to get their human rights; right to privacy is included in article 12(4) in UDHR. No one can violate others privacy.

[17] https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

[18] https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR?amp=1

VIII. REFERENCE:

A. https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR?amp=1
B. https://www.cloudflare.com/learning/privacy/what-is-data-privacy/
C. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
D. https://inforrm.org/2021/12/22/top-10-privacy-and-data-protection-cases-of-2021-a-selection-suneet-sharma/
E. https://www.osano.com/articles/data-privacy-laws
F. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/#:~:text=Personal%20data%20is%20information%20that,cookie%20identifier%2C%20or%20other%20factors