European Economic Letters
ISSN 2323-5233
Vol 14, Issue 4 (2024)
http://eelet.org.uk

# Feasibility of the Implementation of Right to be Forgotten in the Indian Data Backup Standards in the Context of DAPA.

**Anusree Bhowmick[1*], Dr. Aarushi Batra[2]**

[1*]Research Scholar, University of Petroleum and Energy Studies, anusreellb@gmail.com, 0009-0006-2331-4979
[2]Assistant professor, University of Petroleum and Energy Studies, aarushi.batra@ddn.upes.ac.in, 0000-0003-1093-7588

**Abstract**

Irrefutably, India's Digital Data Protection Act has brought an evolution in the realm of digital data protection, ensuring the removal of irrelevant personal data. A data protection board has been set up to process the mechanism. A lot of criticism has come up since its enforcement. Amongst all the most underrated one is the absurdity of implementing the right to be forgotten in the context of Indian data backup standards. The backup data are retrieved once data are destroyed or lost. In the concerned paper author will dive into the Indian digital data removal requirement and its alignment with modern data backup standards. Further, the author will strive to explore the implications of the backup standards, data retention policies, backup mediums, search services, and ERP systems. Through this research researcher will strive to find a solution for implementing the right to be forgotten in the purview of data backup standards.

**Keywords:** The right to be forgotten, Indian Digital Data Protection Act, data backup standards.

## I. Introduction:

The first draft of a law protecting personal data was created in 2018, and in 2019 Personal Data Protection Bill was updated and released. In the 2021 bill, a different section for the right to be forgotten was updated later in 2023 the term “right to erasure” was used instead of right to be forgotten”. The goal of the Digital Data Protection Act is to protect people's privacy by punishing those who violate the legislation. In the age of modern technology, where information is shared instantly, this is indeed a lifesaver. To encounter these altercations Digital Data Protection Act 2023 came up with a consent manager who regulates the consent given by data fiduciaries, sets up a data protection board that receives the data removal requests, and resolves the complaints. In terms of security the right to privacy, the right to access, the right to nominate, the right to data portability, the right to withdraw consent, right to complaint have been recognized. Section 12 of the Digital Data Protection Act 2023 recognizes the right to erasure or remove unnecessary data, which is distinct from the right to be forgotten.

The right to be forgotten is a wider term right to erasure is a part of it. As soon as the right to erasure came to light, many controversies came forth regarding the implementation of the alleged right because of its prominent conflict with the right to freedom of speech and expression and the right to information. Judges often compromise with the right to be forgotten to subsist the existence of the other two rights. Similarly, in the prevalence of stringent data backup systems, the genuine recognition of the right to be forgotten succumbs. Now when the right to erasure is on the plate this is high time to discuss the implications of the backup system on the removal of data which are maintained by the Indian government. The government's data retention policy is directly violated or clashes with the right to erasure or the right to be forgotten. Further author sums up the whole paper in the following manner. Section 1 denotes the actual meaning of the right to be forgotten in terms of the Digital Data Protection Act 2023. Section 2 simplifies the Implication of the technicalities of the data backup process: Section 3 focuses on the existence of intricacies between the Indian data backup strategy and the right to be forgotten. Section 4 elucidates the alignment of data backup standards which applies to all government entities of India. Section 5 emphasizes the Implication of the technicalities of the data archival process: Section 6 analyses the Data Retention Policy of India. Section 7 delineates the Implication of the technicalities of the data archival process: Sec 8 outlines the ERP system and its implication. Finally, in section 9 author strives to find a way forward or the possibility of the implementation of the right to be forgotten in the landscape of the data backup strategy.

**I.A. What is data backup system?**

G2's Summer 2024 Report (IT categories): "Data backup is the practice of duplicating your organization's data to ensure its protection in any type of data loss event"[1]

As per the definition of ISO 27001 data backup process is the process of creating copies of data, software, and systems in order to prevent data loss.[2]

According to the dictionary of the Storage Networking Industry Association (SNIA), the Point In Time copy (PIT copy) is "A fully usable copy of a defined collection of data that contains an image of the data as it appeared at a single instant in time. …Implementations may restrict point-in-time copies to be read-only or may permit subsequent writes to the copy"[3]

Data backup systems can be configured to do transaction log backups in addition to mix-and-match modes between full and incremental backups on a daily, weekly, and monthly basis.

All full/ level 0 backups:

Performing a level 0 backup every day onto a separate volume.

Weekly full, daily level differentials:

Throughout most of the week, data need to be restored from 2 volumes- level 0 and the most recent level differential.

Weekly full, daily levelled backups:

Each changed file gets backed up only once and needs a volume to do a full restore.

Monthly full, daily tower of Hanhoi incremental: Each day's backup is based on the previous day's backup, but with a rotating pattern.[4]

**I. Implication of the technicalities of the data backup process:**

Considering the technicalities of the backup system, and archival system the implementation of the Right to be forgotten does not seem to be very smooth rather it is burdensome and impossible to some extent. In this section, the author has highlighted the tinge of some technical obstacles that make the impossibility prominent.

Data is copied to the staging area before being transferred to the eventual backup destination in terms of the data backup procedure. There is always a second duplicate of each object in the system, either in the storage area or in Tivoli Storage Manager, for every object kept in the staging area. Tivoli Storage Manager will never remove backup files older than their current version. The more requests for data retrieval there are, the more likely someone is to retrieve the data. A document that is kept in an optical jukebox under the control of the Tivoli storage manager is copied to the staging area before being sent to the client upon request.[5] Since the document would then reside on a hard drive rather than a slower optical platter, all further requests for this same document would be processed much more quickly. Aside from that, fundamental backup criteria include preserving at least the past three generations of data, or 28 days' worth.[6]

**II. Indian data backup strategy and right to be forgotten:**

As we have already discussed, the right to be forgotten is a wider term, it ensures the removal of all kinds of data. And it implies the removal of data from all sources so that it cannot be retrieved further. But considering the data backup strategy

[1] Linksquare(2024),G2 grid report for contract lifecycle management, Summer 2024. https://linksquares.com/resources/g2-summer-grid-report-clm/

[2] Achmadi, D., Suryanto, Y., & Ramli, K. (2018, May). On developing information security management system (isms) framework for iso 27001-based data center. In *2018 International Workshop on Big Data and Information Security (IWBIS)* (pp. 149-157). IEEE.

[3] Eugenia Politoua , Alexandra Michotab , Efthimios Alepis , Matthias Pocsc , Constantinos Patsakis,(2018). Backups And The Right To Be Forgotten In The GDPR: An Uneasy Relationship. Computer Law & Security Review 34 (2018) 1247–1257

[4] Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2022). A secured database monitoring method to improve data backup and recovery operations in cloud computing. *BOHR International Journal of Computer Science*, *2*(1), 1-7.

[5] Veena, S., Aravindhar, D. J., Sudha, L., & Aruna, K. B. (2021). An incremental snapshot system using smart backup for persistent disks in cloud.

[6] Scope, N., Rasin, A., Lenard, B., Heart, K., & Wagner, J. (2022, July). Harmonizing privacy regarding data retention and purging. In *Proceedings of the 34th International Conference on Scientific and Statistical Database Management* (pp. 1-12).

which is followed by the Indian government the feasibility of the implementation of the newly recognized right raises a big question. On one hand Digital Data Protection Act 2023 data deletion from all sources where it resides on the other hand government has come up with a data retention policy which is completely a hindrance in the path of successful implementation of the right to be forgotten. There is no specific timeframe in the Digital Data Protection Act within which the data should be removed so far as the right to be forgotten is concerned. In this context, the Indian data backup standards and data retention and archive policy seem to be in contradiction to the newly recognized right i.e. the right to be forgotten.
The backup standard's primary goal is to ensure that regular backup copies of crucial firm data are created safely and reliably, allowing business operations to continue in the event of system failures, natural catastrophes, or data loss. In 2023, the backup policy 1.0 went into effect, and it only applies to Indian government entities. The following are some of the purported standard regulations that violate digital data protection's right to be forgotten:[7]
The government uses a 3-2-1 backup plan to save its data. stating that "three copies of the data in total. Two copies must be stored apart from one another. One copy must be stored offsite." The final "one copy" needs to be kept off-line and separated from the network, in a separate geographic location.
This policy applies to any government-collected and stored data that is overseen and maintained by the Information and eGovernment Authority. The purported strategic plan demonstrates that the backup data is distributed to additional unidentified nations in addition to India.
Indian laws including the Information Technology Act 2000, the Digital Data Protection Act 2023, and guidelines of the Reserve Bank of India, The Telecommunication Act 2023 very specific and strict about the data backup policy. But none of them talks about deletion or edibility of it. Rather Financial institutions are required by guidelines issued by the Reserve Bank of India (RBI) to retain records for a specific amount of time.[8] If backup data is deleted against these standards, regulatory penalties may apply. If the international standard is analyzed ISO 27040, Section 7.4.1., states that "archival storage assumes a write-once, read-maybe access pattern, thus the integrity of the data in the system should be actively checked at regular intervals rather than waiting to when it is read".[9] These guidelines make it obvious that data stored in a backup is neither delible nor edible.

**III. Data Backup Standards:**

In this section, the author presents the data backup standards that India has mostly adopted and followed. India doesn't have a data backup policy. It mostly follows some international standards like ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 22301, and the NIST cyber security framework. The NIST Cybersecurity Framework (CSF) basically emerges from the United States, but it is followed by India as a backup standard.
Organizations use data backup standards as a guide to determine what data should be saved where, on what bandwidth, and for what purposes. The primary problem is data protection or data retrieval during catastrophic events.
In India, several IT standardization bodies are there which regulate respective data backup mechanisms including the Bureau of Indian Standards (BIS), Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), Ministry of Electronics and Information Technology (MeitY), Data Security Council of India (DSCI), Telecom Regulatory Authority of India (TRAI), Ministry of Home Affairs (MHA). They frame data backup standards for the protection of their data assets and cyber security. Apart from that India follows some international cyber security frameworks which include data backup standards as a cybersecurity measure.
The Department of Trade and Industry (DTI) of the United Kingdom is usually the source of ISO/IEC 27001, however, India also commonly uses it as a standard for data backup and cyber security. Regarding information security management systems (ISMS) and more general security measures, this is generally accepted. It specifies a few rubrics as a backup standard, which include:[10]

[7] Information and E-government authority(2023).Backup policy 1.0. Governance & Enterprise Architecture Directorate. https://nea.gov.bh/Documents/BackupPolicy.pdf
[8] Bhat, A. A., Khan, J. I., Bhat, J. A., & Bhat, S. A. (2024). Measuring central bank independence in India–a legal and behavioural case of Reserve Bank of India. *International Journal of Social Economics*.
[9] International standard of information technology, (2015)ISO/IEC 27040:2015(E). https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027040-2015.pdf
[10] International standard of information technology, (2022) ISO/IEC 27001. https://www.iso.org/standard/27001

It requires the firm to set up a backup system for important business functions and to periodically take and test backup copies of data, software, and system images by a backup policy.
• Every electronic access control system needs to keep log reports for a minimum of 10 days and document every action.
• It requires the creation of an adequate backup cycle and the encryption of backup data.
To manage inconsistencies in a cloud environment, it also designates the cloud service provider as the backup provider in the following scenarios:

- how the integrity of the backup will be verified
- for restoration and testing
- use of encryption
- for how the backups are segregated
- for frequency and method of review of backups and recovery procedure.

Backup for Applications Using Cloud-Based Productivity
Both on-site and cloud-based user data are covered by this policy. Ninety days is the backup frequency for incremental backup. It requires data to be retained for a minimum of five years, and that too without being altered.[11] This regulation permits certain exclusions, and the Information and eGovernment Authority has been tasked with identifying and overseeing those exemptions.[12]
NIST Cybersecurity Framework (CSF) is not India's own cyber security framework or data backup standard. It emanates from the United States for cyber security and data backup standards. Before utilizing backups and other restoration assets, RC.RP.03 allows for their verification. Communication to specified internal and external stakeholders regarding the recovery efforts and restoration's advancement is required under RC.CO.03.[13]
The alleged standard prescribes a process of restoration of data:

Application of the Organizational Cybersecurity Risk Strategy

Approved by management

Reviewed

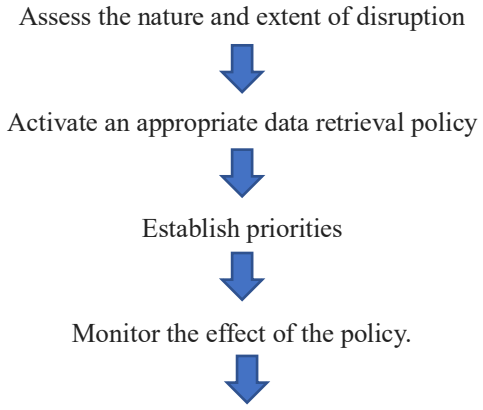
Organization adopts its data backup storage policy based on previous and current cyber security activities

Backup data preservation and retrieval should be routinely shared throughout the organization and with authorized 3rd parties.

Aside from that, the company makes use of real-time or almost real-time information to comprehend and consistently address cybersecurity dangers related to its supplier, as well as the goods and services it purchases and utilizes. To reply successfully, it also requests that you use a consistent approach. Senior cyber security and non-cyber security executives should keep an eye on this.

[11] Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2022). A secured database monitoring method to improve data backup and recovery operations in cloud computing. *BOHR International Journal of Computer Science*, *2*(1), 1-7.
[12] Tello Bahamon, C. C., Claib Meinhardt, A. A., Perez de la Cruz, F., Ramirez Olarte, H. E., Soberanes Hernandez, R. E., Lozano, H. A., ... & Parra, J. (2022, April). Implementation of an Optimized Solution using a Cloud-Based Production Data Management System for Production Operations. In *SPE Western Regional Meeting* (p. D011S002R001). SPE.
[13] National Institute Of Standards And Technology US Department Of Commerce. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

ISO/IEC 22301 is a data backup standard that emphasizes business continuity management systems (BCMS) additionally it provides data availability and data recovery guidelines which include data backup practices. [14]
It prescribes the following guidelines for the data recovery process.




In the case of the backup policy 1.0, the requirements read as follows:[15]
3.2.7. The national cybersecurity center has been given the authority to oversee security management to preserve the authenticity of backup data. to prevent any data from being changed or removed.
3.2.4. There is no specific retention period for normal data. The authority to determine the retention period has been given to the respective government entities and that will be communicated to the Information and eGovernment Authority.
3.2.2. There are daily, monthly, and annual boundaries for the backup frequency. The retention durations are 35 days, 13 months, and 5 financial years for daily, monthly, and annual backup frequency, respectively.

**Table No1**: Annual Data Retention Period of Backup Policy 1.0

| **Backup Frequency** | **Retention Period** |
|---|---|
| Daily | 35 Days |
| Monthly | 13 Days |
| Yearly | 5 Financial years |

Apart from that, the backup policy version 1.0 ensures the following guidelines.

- It requires a backup log of time-stamped data. which requests the saving of information, including the backup date and time. - If the backup was successfully finished. - The reason(s) for the backup's failure, information about the media used for onsite and offshore storage, the backup coordinator(s) for the entity, and the coordinated iGA Department.
- In the event of a disaster, system failure, data loss, data corruption, or depending on unique business requirements, the data must be restored. Additionally, the entity's concerned department(s) as well as the Information and eGovernment Authority should be notified if the restoration procedure fails in any manner.

It is clear from the purported policy and the related regulations that it encourages the maintenance of numerous files containing the same data, either offsite—that is, outside of India—or onsite—that is, in India. In order to protect the data from external intruders, it becomes necessary to store it in an unaltered state. The rules listed above are complicated. There is a clash between the newly established right to be forgotten and the current backup strategy, and one must be sacrificed to support the other. Without changes to the data backup strategy, the right to be forgotten cannot be fully implemented. As a result, companies must coordinate their data backup and deletion procedures, or else they risk serious repercussions.

[14]International organization for standardization.(2019).Business continuity ISO 22301. https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100442.pdf
[15] Information and E-government authority(2023).Backup policy 1.0. Governance & Enterprise Architecture Directorate. https://nea.gov.bh/Documents/BackupPolicy.pdf

## IV. Implication of the technicalities of the data archival process:

Archival data is very crucial for research work, training, and decision-making. This is a prolonged data storage process. because of its cost-effectiveness majority number of people tend to archive data. The cost is comparatively less in comparison to other means.[16] archival storage is allowed to be rescued by the function head of the alleged document, this is not allowed to be accessed in the ordinary course of business. the storage period is determined based on the regulations and business requirements. This is stored for a long period. Recently National Institute of Electronics & Information Technology has introduced a content archival policy in collaboration with the Ministry of Electronics & Information Technology to establish a schedule for the deletion of online data which is of no use. It stipulates a data archival schedule which is as follows:[17]

**Table no2**: Data Archival Schedule by National Institute of Electronics & Information Technology

| **Content Element** | **Exit period** |
|---|---|
| Programs/ Schemes | 5years since the data of discontinuation |
| Government reports and publications | Perpetual since the date of entry into archival |
| Circulars/ Notifications | 5years since the data of discontinuation |
| Photo/ gallery | 5years since the data of discontinuation |
| Highlighted contents | 5years since the data of discontinuation |
| Acts/ Rules | Perpetual since the date of entry into archival |

In addition to that many private companies for their convenience have introduced data archival and retention policies that stipulate that one volume per system per year is kept forever.[18] Files in an archive volume are occasionally preserved indefinitely in accordance with these standards. A company will have 364 copies of many of its files stored on tape if it uses weekly full backups (executing a level 0 backup every day onto a separate volume) or creates archives with its backup product but does not delete the original files and stores its archives for seven years. This ensures long storage of data, even if those files have never changed.[19] The capacity to preserve a stipulated number of copies of an archived item is another important characteristic of the archived system. This augments the complexity of the data deletion process since there is no specific number of copies that could be stored as an archive.[20] Another noticeable problem is that when numerous clients use the same operating system many files of the same category are backed up. this augments the propensity of keeping multiple full backups and multiple duplicate files, which makes the whole data deletion process more complicated.

## V. Analysis of the Data Retention Policy of India:

Data retention refers to a search engine's ability to keep track of previous search query data.[21] The time tenure of data retention depends upon some specific parameters like uniqueness, adequacy of documentation, cost of replacement, and evaluation by peer review. The legal, administrative, fiscal, and evidential value of the record is the main root cause of determining these qualities through which the appraisal is conducted. The appraisal process must apply the established criteria while allowing for the evolution of the criteria and priorities and must be able to respond to special events like when the survival of the data set is threatened. [22]

---

[16] Ringel, S., & Ribak, R. (2021). 'Place a book and walk away': archival digitization as a socio-technical practice. *Information, Communication & Society*, *24*(15), 2293-2306.
[17] Ministry of electronics and information technology (government of india).(2024). National Institute of Electronics & Information Technology. https://www.nielit.gov.in/content/content-archival-policy-cap
[18] Birch, K., Chiappetta, M., & Artyushina, A. (2020). The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset. *Policy studies*, *41*(5), 468-487.
[19] Amos, R., Acar, G., Lucherini, E., Kshirsagar, M., Narayanan, A., & Mayer, J. (2021, April). Privacy policies over time: Curation and analysis of a million-document dataset. In *Proceedings of the Web Conference 2021* (pp. 2165-2176).
[20] Hunter, G. S. (2020). *Developing and maintaining practical archives: A how-to-do-it manual*. American Library Association.
[21] Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (2023). Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*, *29*(1-2), 176-211.
[22] Fizur, E. (2020). *Long term data retention* (Doctoral dissertation, Rutgers University-Camden Graduate School).

Generally, all data that are useful, nonredundant, and documented well enough for most primary uses should be permanently maintained.

According to the NCL_Data Retention Archival Policy - V1.0 retention is defined as "the maintenance of documents in a live environment which can be accessed by an authorized user in the ordinary course of business".[23] Many supporters argue that to obtain high-quality searches, data preservation is essential. The length of time that data must be kept in any organization or the maximum period that it can be erased is not specified in the recently passed Digital Data Protection Act 2023. It only states that "A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force, erase personal data, upon the Data Principal withdrawing her consent".[24]

Although data retention is required by various statutes in Indian law, which do not expressly address retention policies, noncompliance can result in damages.

The Companies Act of 2013 mandates that certain types of records, such as the company's financial statements, annual reports, and books of accounts, be kept on file for a maximum of eight (8) years or indefinitely in India. Failure to do so demands a fine of Rs. 50,000.[25]

Regulation 9 of the Securities Exchange Board of India Regulations 2015 allows for an eight-year document preservation period.[26] In addition, central labor laws like the Payment of Gratuity Act of 1972, the Equal Remuneration Act of 1976, the Minimum Wages Act of 1948, and the Payment of Wages Act of 1936 mandate the maintenance of combined employee registers for workers that include personal data like name, date of birth, address, phone number, educational background, and bank account numbers.

The Income Tax Act of 1961 allows the income tax authorities to call for the books of account or reopen any tax assessment for a total of eight (8) years, or six (6) years following the conclusion of the relevant assessment year. Ten thousand rupees in damages are imposed for every failure.[27]

Any entity that collects an individual's Aadhaar number is required to maintain the security and confidentiality of that information, including any database in which that information is stored, under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (the "Aadhaar Act") and Aadhaar (Sharing of Information) Regulations, 2016 (the "Aadhaar Regulations"). A violation of it carries a penalty of Rupees Twenty-Five Thousand (INR 25,000) or, in the case of a firm, Rupees One Hundred Thousand (INR 100,000) in jail for a maximum of one (1) year.[28]

Prevention of Money Laundering Act (PMLA), 2002 requires that records of all transactions be kept for at least five (5) years from the date of the transactions, and that client identification records be kept for five (5) years after the end of the business relationship.[29] The Indian Telegraph Act 1885 requires operators to retain documents for a year.

Banks are also required to keep certain registers (like ledgers about loans, remittances, overdrafts, etc.) and other documentation (like pay-in slips, vouchers, paid checks, etc.) for eight (8) years under the Banking Companies (Period of Preservation of Records) Rules, 1985.

In the year 2012, a data retention schedule was proposed by the Government of India concerning records common to all ministries and departments. Which stipulates certain retention periods of government documents are as follows:

[23]NSE Clearing. (2023). NCL_Data Retention Archival Policy - V1.0. Data_RA/001. https://www.nsccindia.com/sites/default/files/disclosure-doc/202401/NCL_Data%20Retention%20%20Archival%20Policy%20-%20V1.pdf

[24] The Digital Personal Data Protection Act, 2023, 22 DPA S 8 (2023). https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[25]The Companies Act, 2013, 18 CA S128 (2013). https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf

[26] Income Tax Act of 1961, 43 ITA S 148A. https://cleartax.in/s/notice-section-148-income-tax-act

[27] The Aadhaar Act, 2016, 47 S 38. https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

[28]The Reserve Bank of India Act, 2 RBI S. https://www.indiacode.nic.in/bitstream/123456789/2398/1/a1934-2.pdf.

[29]The Reserve Bank of India Act, 2 RBI S 45K 45L. https://www.indiacode.nic.in/bitstream/123456789/2398/1/a1934-2.pdf.

[29] Prevention of Money Laundering Act (PMLA), 2002. 15 PML S 12(1). https://www.indiacode.nic.in/bitstream/123456789/15402/1/moneylaunderingact2002.pdf

**Table No.3** Data Retention Period of Government Document Scheduled by Government of India

| | |
|---|---|
| **Records Retention Schedule of Employment & Training**[30] | |
| Collection of Statistical Data on Apprentices at State/Central level. | B |
| Court cases regarding Apprenticeship Training etc. | C-3 (3 years after the final judgment of the court under the normal course of law) |
| Files for employers | C3 (3 years after the final judgment of the court under the normal course of law) |
| Court cases regarding information marketing information | C-3 (3 years after the final judgment of the court under the normal course of law) |
| Appeals/ Court cases regarding training craftsman desk | C-3 (3 years after the final judgment of the court under the normal course of law) |
| **Retention Schedule of Water Resources** | |
| Policy matters relating to any issue/organization | B Keep (data preserved for extended duration) |
| Records Relating to Technical Aspects of Inter-State River Water Disputes | B Keep (data preserved for extended duration) |
| Appeals/ Court cases | C-3 (3 years after the final judgment of the court under the normal course of law) |
| **Retention Schedule of Ministry of Electronics and Information Technology (MeitY)** | |
| Policy Matters | B |
| Management Records | C5 (5 years) |
| Customer Related Records | C10 (10 years) |
| | |
| Personal files or documents | C5(5 years) |
| **Data Retention Schedule for Civil Aviation** | |
| RTI Cases Attracting 2nd Appeal (without any remarkable decision) | C3(3Years) |
| RTI Cases attracting 2nd Appeal (involving a remarkable decision) | C5(5 years) |
| Appeal cases | C3 (3Years) |
| Files relating to the administrative aspects of RTI Act, 2005 | C3 (3Years) |
| Register of RTI Applications | B Keep (long-term retention) |
| **Retention of Railway Data** | |
| Arbitration and litigation cases. | 3Years |
| Court cases | 10 years |
| Appeals | 10 years |

## VI. Content management system and it's implication:

Because of the emergence of digitalization, content management system has engrossed into every sector to manipulate content production, delivery and handling. The predominant objective of the content management system to simplify the

[30] Joshi R, (2016) Record retention schedule for records relating to substantive function. (Report NoI34011/07/2005IWSU).MinistryofLabour&Employment.https://labour.gov.in/sites/default/files/recordretentionscheduledget.pdf

handling and usage of the broadcasting and archiving.[31] So far as the content management system is concerned the most crucial task is to maximize the potential of the reuse of present material and minimize the expense of production. This is basically accomplished by providing easy access via intuitive user interfaces, feedback to searches and vital element of human machine interaction.[32] Through computer-based content analysis, content management systems offer capabilities of automatically extracting data from the content itself. The primary goal of a content management system is to automatically produce as much metadata as possible to streamline documentation and reduce the need for human involvement.[33] The digitized content supported by the content manager includes HTML, XML-based web content, images, electronic official documents, and rich media such as digital audio and video.[34] In the media sector to manage digital media assets the content management system has been prioritized that provides new ways of collaboration, communication, and commercial exploitation of content. In this system restoration and achieving data become integral in the process of integration of application and management of content.[35] The information specifically the case information including crime type, date, location case number, suspect criminal data including the name of the concerned person, images, prior criminal history, employment, arrest information, and court proceedings. Apart from that victim's identity, the victim's background, and the impact of crime. Multimedia and supporting content including images and footage related to crime scenes, visual representation of crime data, and information on other crimes that might be similar or connected to the crime.[36]

**Table No.4:** The Data Stored in Content Management System

| | |
|---|---|
| Crime type | Employment |
| Date of the commission of crime | Arrest information |
| Case number | Court proceeding |
| Name of the concerned person | Victim's identity |
| Images | Victim's background |
| Prior criminal history | Visual representation |

## VII. ERP system and its implication:

The main purpose of an ERP system is to integrate and streamline an organization's core business processes into a unified system through the processing of information and amalgamation of best practices together.[37] To maintain appropriate security control ERP system ensures accessibility of data so that employees can easily access use and retrieve the data. Likewise, when new employees are recruited using the ERP process some personal data of the employee are stored and

[31] Strekalova, Y. A., & Bouakkaz, M. (2022). Content Management System (CMS). In *Encyclopedia of Big Data* (pp. 208-211). Cham: Springer International Publishing.
[32] Santos, A. S. P., Vieira, J. M. P., Lima, M. A. D. M., Soares, S. R. A., Pereira, L. V., Sampaio, V. M. P., Araujo, B. M. (2024). A technical–scientific content management system on water reuse as an environmental education tool: the experience of a Portugal/Brazil partnership. *Water Supply*, ws2024214.
[33] Shurak, A. D., & Tikhonov, D. V. (2021). Optimizing the content of the educational organization's community in order to expand the target audience. *St. Petersburg State Polytechnical University Journal. Humanities and Social Sciences*, *12*(2), 54.
[34] Brockhaus, J., Buhmann, A., & Zerfass, A. (2023). Digitalization in corporate communications: understanding the emergence and consequences of CommTech and digital infrastructure. *Corporate Communications: An International Journal*, *28*(2), 274-292.
[35] Lutfiani, N., Rahardja, U., & Khasanah, K. T. (2022). The development viewboard as an information media at official site asosiation. *APTISI Transactions on Management*, *6*(1), 10-18.
[36] Javed, U., Shaukat, K., Hameed, I. A., Iqbal, F., Alam, T. M., & Luo, S. (2021). A review of content-based and context-based recommendation systems. *International Journal of Emerging Technologies in Learning (iJET)*, *16*(3), 274-306.
[37] Rankinen, J. (2022). *ERP system implementation* (Master's thesis, J. Rankinen).

retrieved to facilitate and take the process forward.[38] Including full name, contact details, resume/CV all crucial information are provided. For reference, a list providing all necessary information is referred to below in Table 5.

**Table No. 5:** The Data Stored in Content Management System

| | |
|---|---|
| **Name** | **Risk assessment** |
| **Contact details** | **Financial sector check** |
| **Bank account details** | **Pending legal cases** |
| **Previous conviction report** | **Health details** |
| **Arrest record** | |
| **Government security clearance level** | |

Similarly, when media reports on a crime and a criminal within an Enterprise resource planning process some personal data are to be restored and retrieved. Including crime details, suspects' personal information, victim's information, and witness information.[39]

The purpose of entering this data is to use the ERP process, which will be used throughout the ERP packages, to maintain the standards set in every area. To create a single new item in the ERP program, about 150 data fields must be filled up.[40] Generating data, restoring, and retrieving data are quintessential to process the whole ERP process. In this context request for the removal of data in compliance with sec 12 of the Digital Data Protection Act 2023 collides with the main ethics of the ERP system.

The main objective of enterprise resource planning is to combine all available data into a single source. The flow of information becomes fragmented and tends to spread to other systems and externalities. It reduces the possibility of the right to be forgotten being properly executed since, as it grows, it becomes impossible to remove data from all sources used by each organization.[41]

Hence in brief to maintain the ethics of the ERP system in every sphere preservation restoration and retrieval of data is quintessential whereas the removal of irrelevant data is the heart of the right to be forgotten or the right to erasure. It clashes with each other's principles and its implementation.

## VIII. Conclusion & Suggestion:

Digital Data Protection Act 2023 comes up with many rights that helm human rights including some fundamental rights but legislators have failed to consider the strategy or technicality. Companies strive to resort to modern technical systems to smoothen the process or make the process productive, which includes Enterprise Resource Planning, Document management systems, content management systems, enterprise asset management systems, etc. All these systems lead to the preservation, restoration, and retrieval of data. In this context, the removal of data becomes impossible since the data

[38] Tarigan, Z. J. H., Suprapto, W., Harjanti, D., Malelak, M. I., & Basana, S. R. (2021). *Key user ERP capability maintaining ERP sustainability through effective design of business process and integration data management Key user ERP capability maintaining ERP sustainability through effective design of business process and integration data management* (Doctoral dissertation, Petra Christian University).

[39] Han, T., Xiu, L., & Yu, G. (2020). The impact of media situation on people's memory effect--an ERP study. *Computers in Human Behavior*, *104*, 106180.

[40] Fan, B., Liu, S., Pei, G., Wu, Y., & Zhu, L. (2021). Why do you trust news? The event-related potential evidence of media channel and news type. *Frontiers in Psychology*, *12*, 663485.

[41] Baum, J., & Abdel Rahman, R. (2021). Emotional news affects social judgments independent of perceived media credibility. *Social Cognitive and Affective Neuroscience*, *16*(3), 280-291.

is not only stored in the concerned company but circulated in different companies for data integration. Which directly clashes with the main principle of the right to be forgotten or the right to erasure. Apart from that complying with different backup policies and data retention policies becomes a big question in the way of the implementation of the right to be forgotten and the right to erasure. To get rid of problems like data loss and other disasters maintaining data backup and its time-to-time retrieval becomes important to maintain the organizational protocol. Taking all these rubrics into consideration execution of data removal becomes very challenging. Henceforth the principles alluded to in the Digital Data Protection Act 2023 including the right to be forgotten must be aligned to the organizational technicalities and other ancillary protocols that augment the feasibility of the execution of the alleged newly recognized right.

When the right to be forgotten is being implemented deletion of data from the database is just an eyewash since it remains there in the backup. Many data backup policies that India presently follows inanimate the edibility of data stored in data backup. Some of them mandate to keep data forever. This forcibly preserves data. Hence a flexible data backup mechanism should be formulated that allows to removal of data not only from the database but also from data backup storage. Hence deletion of data from all sources and means must be ensured.

Since several copies of backup data are stored onsite and offsite, it might be difficult to find the file unless the location of the file is exactly known. Encryption of the backup data could be one of the solutions. The key should be accessed by the data principal, and members of the data protection board.

Chapter VI, sec 27 of the data protection act 2023 provides the power of the data protection board which includes the inquiry of the request of data deletion, and data breach. The data protection board should take charge of the data stored in data backup as well in collaboration with the consent manager.

There should be a separate provision containing a schedule for regular testing of backups. Which will push organizations to check the data removal requests in scheduled frequency from data backup as well.

Section 12 of the digital data protection act 2023 only provides direction for data removal which is recognized as the right to erasure but there is no limitation or deadline of the removal of data neither from the database nor from backup data storage. There should be a proper deadline for data removal from the database and from backup data storage.

**References:**

1. Linksquare(2024),G2 grid report for contract lifecycle management, Summer 2024. https://linksquares.com/resources/g2-summer-grid-report-clm/
2. Achmadi, D., Suryanto, Y., & Ramli, K. (2018, May). On developing information security management system (isms) framework for iso 27001-based data center. In *2018 International Workshop on Big Data and Information Security (IWBIS)* (pp. 149-157). IEEE.
3. Eugenia Politoua , Alexandra Michotab , Efthimios Alepis , Matthias Pocsc , Constantinos Patsakis,(2018). Backups And The Right To Be Forgotten In The GDPR: An Uneasy Relationship. Computer Law & Security Review 34 (2018) 1247–1257
4. Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2022). A secured database monitoring method to improve data backup and recovery operations in cloud computing. *BOHR International Journal of Computer Science*, *2*(1), 1-7.
5. Veena, S., Aravindhar, D. J., Sudha, L., & Aruna, K. B. (2021). An incremental snapshot system using smart backup for persistent disks in cloud.
6. Scope, N., Rasin, A., Lenard, B., Heart, K., & Wagner, J. (2022, July). Harmonizing privacy regarding data retention and purging. In *Proceedings of the 34th International Conference on Scientific and Statistical Database Management* (pp. 1-12).
7. Information and E-government authority(2023).Backup policy 1.0. Governance & Enterprise Architecture Directorate. https://nea.gov.bh/Documents/BackupPolicy.pdf
8. Bhat, A. A., Khan, J. I., Bhat, J. A., & Bhat, S. A. (2024). Measuring central bank independence in India–a legal and behavioural case of Reserve Bank of India. *International Journal of Social Economics*.
9. [1]International standard of information technology, (2015)ISO/IEC 27040:2015(E). https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027040-2015.pdf
10. International standard of information technology, (2022) ISO/IEC 27001. https://www.iso.org/standard/27001

11. [1] Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2022). A secured database monitoring method to improve data backup and recovery operations in cloud computing. *BOHR International Journal of Computer Science*, *2*(1), 1-7.
12. Tello Bahamon, C. C., Claib Meinhardt, A. A., Perez de la Cruz, F., Ramirez Olarte, H. E., Soberanes Hernandez, R. E., Lozano, H. A., ... & Parra, J. (2022, April). Implementation of an Optimized Solution using a Cloud-Based Production Data Management System for Production Operations. In *SPE Western Regional Meeting* (p. D011S002R001). SPE.
13. National Institute Of Standards And Technology US Department Of Commerce. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
14. [1]International organization for standardization.(2019).Business continuity ISO 22301. https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100442.pdf
15. Ringel, S., & Ribak, R. (2021). 'Place a book and walk away': archival digitization as a socio-technical practice. *Information, Communication & Society*, *24*(15), 2293-2306.
16. [1] Ministry of electronics and information technology (government of india).(2024). National Institute of Electronics & Information Technology. https://www.nielit.gov.in/content/content-archival-policy-cap
17. Birch, K., Chiappetta, M., & Artyushina, A. (2020). The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset. *Policy studies*, *41*(5), 468-487.
18. [1] Amos, R., Acar, G., Lucherini, E., Kshirsagar, M., Narayanan, A., & Mayer, J. (2021, April). Privacy policies over time: Curation and analysis of a million-document dataset. In *Proceedings of the Web Conference 2021* (pp. 2165-2176).
19. [1] Hunter, G. S. (2020). *Developing and maintaining practical archives: A how-to-do-it manual*. American Library Association.
20. [1] Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (2023). Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*, *29*(1-2), 176-211.
21. Fizur, E. (2020). *Long term data retention* (Doctoral dissertation, Rutgers University-Camden Graduate School).
22. [1]NSE Clearing. (2023). NCL_Data Retention Archival Policy - V1.0. Data_RA/001. https://www.nsccindia.com/sites/default/files/disclosure-doc/202401/NCL_Data%20Retention%20%20Archival%20Policy%20-%20V1.pdf
23. The Digital Personal Data Protection Act, 2023, 22 DPA S 8 (2023). https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
24. [1]The Companies Act, 2013, 18 CA S128 (2013). https://www.mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf
25. [1] Income Tax Act of 1961, 43 ITA S 148A. https://cleartax.in/s/notice-section-148-income-tax-act
26. the Aadhaar Act, 2016, 47 S 38. https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf
27. [1] The Reserve Bank of India Act, 2 RBI S . https://www.indiacode.nic.in/bitstream/123456789/2398/1/a1934-2.pdf.
28. [1] The Reserve Bank of India Act, 2 RBI S 45K 45L. https://www.indiacode.nic.in/bitstream/123456789/2398/1/a1934-2.pdf.
29. [1] Prevention of Money Laundering Act (PMLA), 2002. 15 PML S 12(1). https://www.indiacode.nic.in/bitstream/123456789/15402/1/moneylaunderingact2002.pdf
30. Joshi R,(2016) Record retention schedule for records relating to substantive function. (Report No I34011/07/2005IWSU).MinistryofLabour&Employmenthttps://labour.gov.in/sites/default/files/recordretentionscheduledget.pdf
31. Strekalova, Y. A., & Bouakkaz, M. (2022). Content Management System (CMS). In *Encyclopedia of Big Data* (pp. 208-211). Cham: Springer International Publishing.
32. [1] Santos, A. S. P., Vieira, J. M. P., Lima, M. A. D. M., Soares, S. R. A., Pereira, L. V., Sampaio, V. M. P., Araujo, B. M. (2024). A technical–scientific content management system on water reuse as an environmental education tool: the experience of a Portugal/Brazil partnership. *Water Supply*, ws2024214.
33. [1] Shurak, A. D., & Tikhonov, D. V. (2021). Optimizing the content of the educational organization's community in order to expand the target audience. *St. Petersburg State Polytechnical University Journal. Humanities and Social Sciences*, *12*(2), 54.

34. Brockhaus, J., Buhmann, A., & Zerfass, A. (2023). Digitalization in corporate communications: understanding the emergence and consequences of CommTech and digital infrastructure. *Corporate Communications: An International Journal*, *28*(2), 274-292.
35. [1] Lutfiani, N., Rahardja, U., & Khasanah, K. T. (2022). The development viewboard as an information media at official site asosiation. *APTISI Transactions on Management*, *6*(1), 10-18.
36. [1] Javed, U., Shaukat, K., Hameed, I. A., Iqbal, F., Alam, T. M., & Luo, S. (2021). A review of content-based and context-based recommendation systems. *International Journal of Emerging Technologies in Learning (iJET)*, *16*(3), 274-306.
37. [1] Rankinen, J. (2022). *ERP system implementation* (Master's thesis, J. Rankinen).
38. Tarigan, Z. J. H., Suprapto, W., Harjanti, D., Malelak, M. I., & Basana, S. R. (2021). *Key user ERP capability maintaining ERP sustainability through effective design of business process and integration data management Key user ERP capability maintaining ERP sustainability through effective design of business process and integration data management* (Doctoral dissertation, Petra Christian University).
39. [1] Han, T., Xiu, L., & Yu, G. (2020). The impact of media situation on people's memory effect--an ERP study. *Computers in Human Behavior*, *104*, 106180.
40. [1] Fan, B., Liu, S., Pei, G., Wu, Y., & Zhu, L. (2021). Why do you trust news? The event-related potential evidence of media channel and news type. *Frontiers in Psychology*, *12*, 663485.
41. Baum, J., & Abdel Rahman, R. (2021). Emotional news affects social judgments independent of perceived media credibility. *Social Cognitive and Affective Neuroscience*, *16*(3), 280-291.