Deloitte.

blancco

Data Destruction Survey Report

For Private circulation only

2020

This draft document is subject to the firm’s internal clearances per its internal policies and processes such as independence and conflict check, etc.

Foreword

The digital transformation of enterprises has paved the way for a data-centric ecosystem. Globally, there is a shift in the maturity of information management models. With advancements and new developments in information and data management technologies, the data-centric ecosystems across the world have experienced enforcement of several regulations. With the increase in evolving business models, standardised frameworks, and operational maturity of organisations, India is considered as one of the key providers of technology and services.

Along with the transition from traditional IT infrastructure to virtualised and remotely managed systems, organisations must understand how to protect data in the most appropriate manner towards the end of the data lifecycle. The two critical end stages are the Archive stage, which addresses retention policies and adherence with those policies, and the Dispose stage, which addresses end-of-life data sanitisation of assets or from within active environments. However, new laws and regulations are specifying what should happen once data retention dates expire. These requirements are usually based on the data's confidentiality classification.

Proactively addressing the above-mentioned stages ensures that data policies continue to be enforced throughout the organisation in a manner that ensures that data is irrecoverable upon destruction.

Blancco (Software) India Private Limited (Blancco India) and Deloitte Touché Tohmatsu India LLP (DTTILLP, or Deloitte) jointly conducted the *Blancco-Deloitte Data Destruction Survey 2020* from December 2019 through January 2020. This included identifying the level of awareness and maturity of organisations regarding data sanitisation and retention requirements, which is established by relevant regulations and guidelines and how they are currently addressing the issue. The survey results constitute the inputs of 60 respondents from various sectors. The survey results aim to provide an understanding of the adoption of data erasure practices by Indian organisations.

This report provides an overview of the current data retention and disposal practices in Indian organisations.

About Blancco
Blancco is the industry standard in data erasure and mobile device diagnostics software. Blancco's data erasure software provides thousands of organisations the tools they need to enable sustainable data sanitisation processes across the widest array of IT assets. By focusing on erasing and reusing assets instead of physically destroying them, organisations can improve their security posture and address corporate social responsibility requirements, while also ensuring compliance with local and global data privacy requirements.

Blancco data erasure solutions have been tested, certified, approved, and recommended by 15+ governing bodies and leading organisations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities, and independent testing laboratories. All Blancco erasures are verified and certified, resulting in a tamper-proof audit trail.

About Deloitte
Deloitte Touché Tohmatsu India LLP (DTTILLP or Deloitte) is one of the world's largest and most diversified professional services organisations, providing assurance & advisory, tax, management consulting, and enterprise risk management services through more than 2,86,200 professionals in more than 150 countries. Our organisation includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touché Tohmatsu India LLP (DTTILLP) is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate.

In India, Deloitte is recognised as one of the country's top professional services firms, with over 12,000+ professional staff. Our professionals are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments.

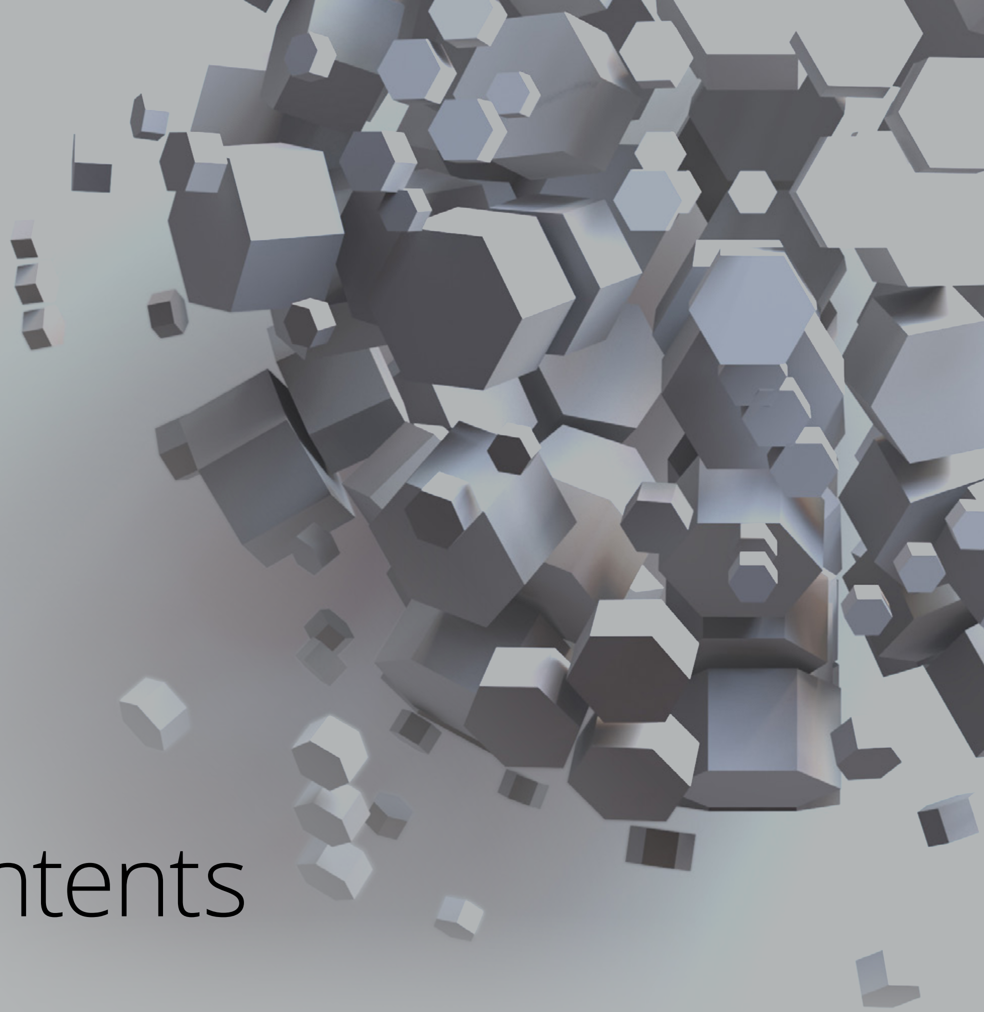


Table of Contents

Executive summary

Around the world, many countries hold organisations responsible for effective sanitisation at the end-of-data lifecycle, especially the ones collecting and processing personal data. The end-of-life of data may be determined by multiple data processing grounds, such as fulfilment of purpose, validity of consent, etc. This accountability lies with the organisation that collects personal data, and also business partners (including vendors, third parties, subcontractors, etc.) who store or process the data. The efficient management of data from its inception through its disposition is the responsibility of all organisations handling the data.

The Blancco-Deloitte Data Destruction Survey was conducted to obtain insights into the practices of organisations related to data retention, erasure, and destruction policies.

The survey noted key aspects related to data retention and destruction, including awareness, compliance, team formation, and major challenges. One of the key drivers for organisations to investigate their end-of-life of data practices were privacy regulations and laws. The survey results identified the leading privacy drivers as the General Data Protection Regulation (GDPR), ISO 27001 (Information Security Management System standard), and draft Personal Data Protection Bill 2019 (draft PDPB 2019) (1.1 Insight). The data retention and destruction practices followed by the organisations help them with compliance to the aforementioned laws, shrink attack surface, and enhance security.

Amongst the organisations surveyed, 87 percent have begun their journey towards readiness with respect to data privacy regulations. They initiated their journey by either assessing their posture against current privacy laws or complying with privacy requirements (3.1 Insight).

If we break it down further, Business-to-Business (B2B) organisations (39 percent) are ahead in their journey, having implemented privacy requirements per applicable privacy laws. By contrast, the journey for business-to-consumer (B2C) organisations has just begun (22 percent, 3.2 Insight). More than 20 percent of the large organisations (more than 10,000 employees) are completely unaware of the current and upcoming laws and regulations around privacy (2.2 Insight), according to the survey.

The European Union's GDPR and India's draft PDPB 2019 place restrictions on the time span for organisation's to retain personal data. They also require organisations to respect the rights of data subjects, such as the 'right to be forgotten.' The aforementioned requirements of relevant regulations require organisation-wide awareness of ways to dispose off data so that it cannot be recovered. This will be supported by gaining visibility into outsourced data destruction practices.

The GDPR and draft PDPB 2019 also mandate that organisations should have a Data Protection Officer (DPO). The survey also covered the aspect of establishing a core privacy team to support this DPO. Large organisations (with 10,000 or more employees) are more likely to have, or intend to, appoint a DPO than smaller organisations (500-1,000 employees) (3.4 Insight). The privacy team may take up the responsibility to set up a comprehensive data retention policy and a robust privacy programme. The benefits of a well-implemented data retention policy and programme can include stringent data protection and updating the data.

The report concludes by highlighting major challenges for data disposal when data reaches the end of its retention period, usefulness, or other condition requiring its sanitisation. It is a critical requirement for organisations to ensure the efficacy of their data disposal techniques. With more stringent data privacy laws in place, secure and certified methods of data destruction are required to support enterprise compliance and compliance by third-party vendors.

01
Introduction

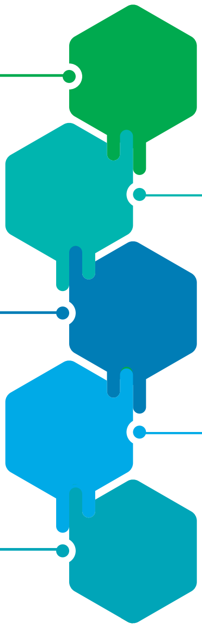
Background

The new and evolving categories of personal data are altering the application of regulatory requirements and the storage dynamics in various industries. Privacy and management of this data pool throughout its lifecycle is fast becoming a core business mandate. Without the right data retention and long-term archiving solutions, efforts to manage the data lifecycle can become futile. Storing data beyond its mandated retention period makes an organisation more vulnerable to a data breach or regulatory non-compliance, which may have an impact in many forms, including but not limited to financial and/or reputational loss. The correct technology implementations can lower data management and retention costs, along with organisational risks, in both the short and long run.

With an increase in privacy laws, the requirements for personal data protection, including data retention and erasure, has become a concern for all organisations. Its scope goes far beyond knowing what data to retain and for what time. The Generally Accepted Privacy Principles (GAPP) also highlights that the entity shall retain personal data for only as long as necessary to fulfil the stated purposes or as required by law or regulations and thereafter, appropriately dispose of such data. Due to these privacy laws or regulations, individuals have become more aware and observant of the privacy notices, policies, and personal data that they provide organisations.

It is recommended that the organisations look at leading practices related to data management all along the data lifecycle, including retention and disposal. Data must be permanently destroyed to prevent restoration, which can be verified through a certificate of data sanitisation.

For the ease of reading this report and to gain more clarity into the practices of an organisation, the terms *data disposal, data destruction, data sanitisation, data erasure,* and *data deletion* are defined as follows:[1]



Data disposal

Data disposal is the general term that refers to data destruction processes. It is also the final stage in the data lifecycle.

Data destruction

Under data disposal, *data destruction* is the process of destroying data from digital storage media so that it is completely unreadable and cannot be accessed or used for unauthorised purposes. It can be achieved digitally or physically, but does not necessarily verify that no usable residual data resides on the storage media. This survey investigates the various methods and approaches that India's enterprises use to destroy data when it has reached the end of its usable life.

Data sanitisation

Data sanitisation is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable, even with the assistance of advanced forensic tools. It can be achieved through *physical destruction* (renders the device unusable), *cryptographic erasure* (relies on encryption software and cryptographic keys), and *data erasure,* with each method having its own advantages and disadvantages.

Data erasure

Data erasure is the software-based method of securely overwriting data from any data storage device using zeros and ones onto all sectors of the device, then verifying and certifying the erasure. By overwriting the data on the storage device, the data is rendered unrecoverable and achieves data sanitisation. With data erasure, the data storage device can still be used (in contrast to physical destruction).

Data deletion

With *data deletion,* the pointers to the data are removed and the data is hidden, but the data is recoverable from the storage device using data recovery tools. This indicates that mere data deletion is an inadequate method of protecting end-of-life data, and fails to comply with data disposal requirements.

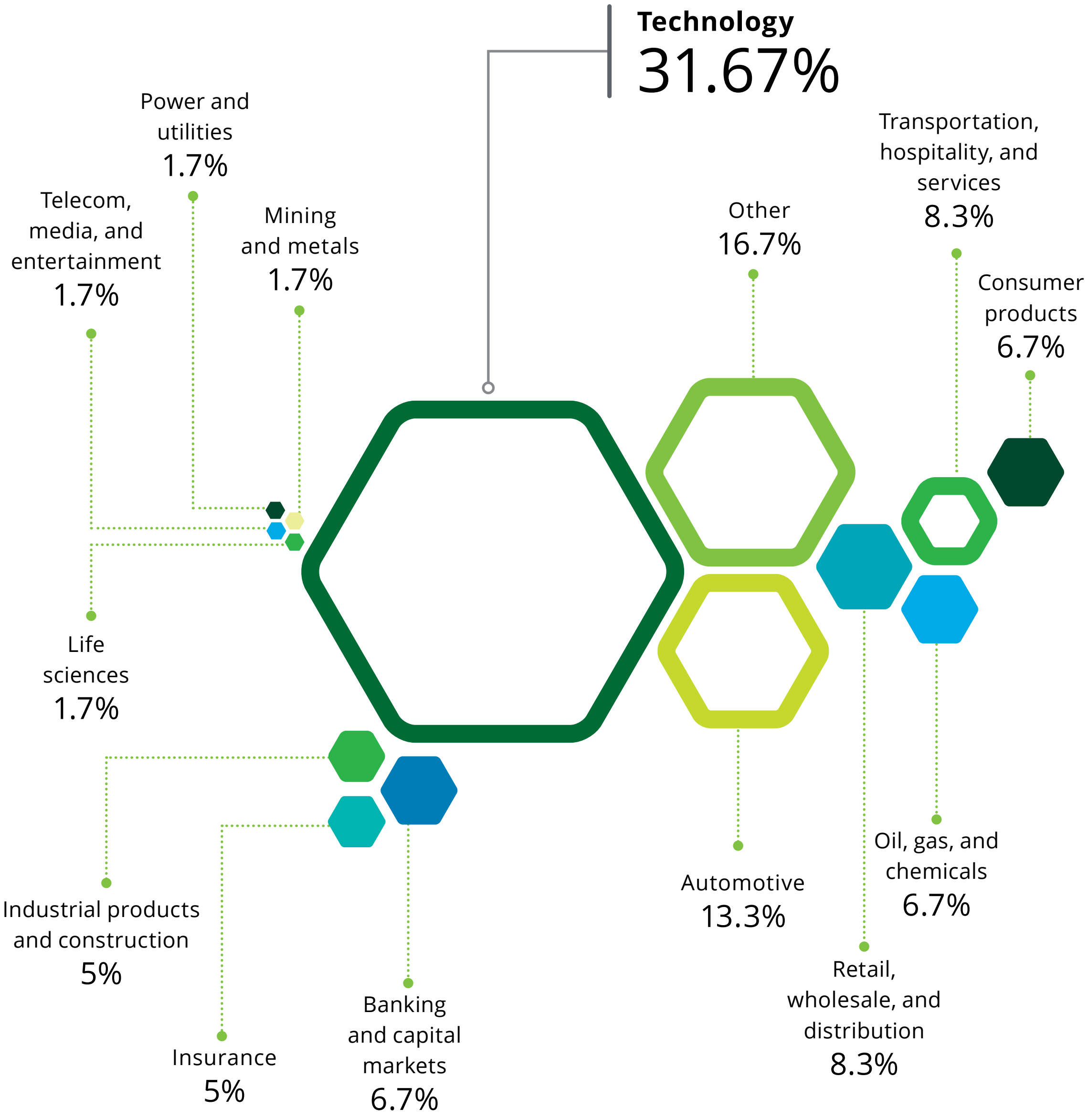
[1] Data Sanitization Terminology and Defnitions (www.datasanitization.org/data-sanitization-terminology/), International Data Sanitization Consortium (IDSC)

Objective

The survey aimed to assess the adoption of data erasure practices by Indian organisations. This included gaining insights on the following:

- Identifying the final stages of the data lifecycle, the relationship between retention and disposal, and timelines for data disposal
- Data retention and sanitisation requirements established by relevant privacy regulations and guidelines
- Awareness and maturity of data end-of-life, data expiry, and related destruction methods
- Current data retention policies and leading practices for data destruction
- Challenges organisations face in implementing data disposal requirements

Response distribution by sector



Methodology

A comprehensive methodology was used to design the survey report and obtain insights. The first step consisted of secondary research about data lifecycle management, retention, destruction, and sanitisation and the second step was to prepare and roll out the survey for two months. The responses obtained from the 60 participants were considered as part of the primary research. The detailed findings were then combined with secondary research to derive insights on data retention, destruction, sanitisation practices, and the management of data throughout its lifecycle.

Survey participants

The survey participants were from a variety of sectors (such as technology, automotive, insurance, and retail) and industries such as technology, media, automotive, insurance, consumer, government and public services, financial, energy resources and industrials and life sciences and healthcare.

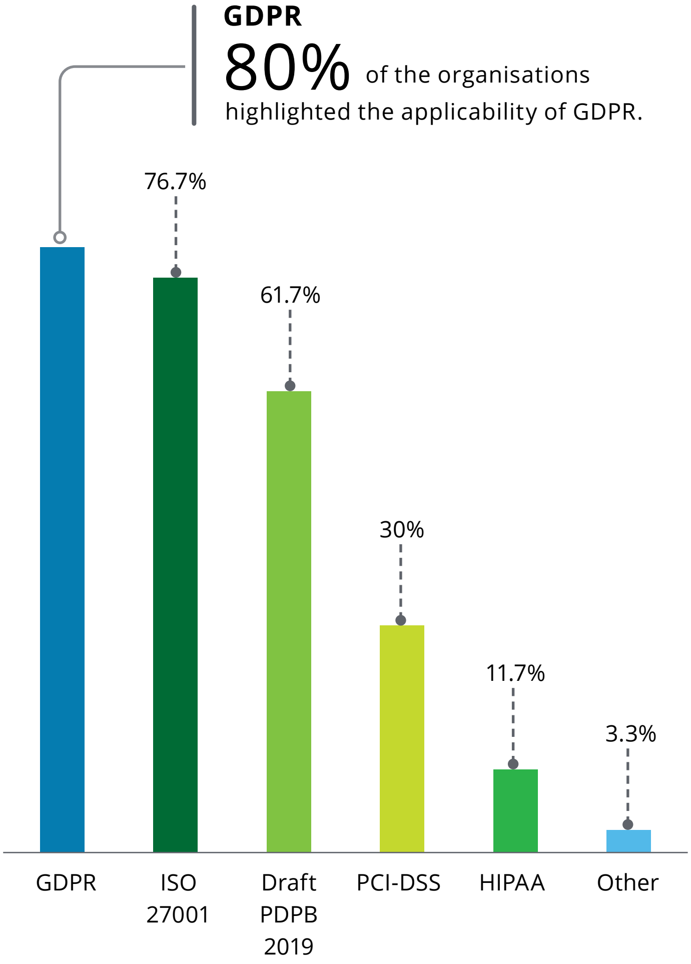
Approximately one third of the respondents belonged to the technology sector.

According to the survey, 15 percent of the respondents represented B2C businesses, and around 38 percent represented B2B.

1.1 Insight: Amongst various privacy standards, laws, and regulations across the world, 80 percent of the organisations highlighted the applicability of GDPR. The remaining identified laws, regulations, and standards (such as ISO 27001), draft PDPB 2019, PCI–DSS (Payment Card Industry Data Security Standard), and HIPAA (Heath Insurance Portability and Accountability Act) as the key drivers of organisational data privacy measures. India's draft PDPB 2019 and laws from many countries took the GDPR as a guideline, and the draft PDPB 2019 emulates the privacy principles to be incorporated under GDPR. Survey responses indicate that laws that have higher penalties and strict compliances are widely adopted (93 percent of the respondents indicate applicability of laws). In addition, industries seek frameworks and standards to improve their privacy posture. This is confirmed by 83 percent of the respondents.

GDPR

80% of the organisations highlighted the applicability of GDPR.



02

Organisational awareness of data retention and data disposal

Awareness on data retention and disposal

The Asia Pacific region is home to some of the world's fastest growing businesses. Multinational organisations in the Asia Pacific region also move data across borders to serve customers in a global digital economy. Per *The Asia Pacific Privacy Guide, Deloitte-July 2019*[2], 15 out of the 21 countries in this region have laws regarding data retention and destruction that mandate regularly updating personal data, making sure it is complete, accurate, and not keeping it longer than necessary. If the data is no longer required for a particular purpose, it should be securely destroyed and/or de-identified.

The following table depicts the aspects of privacy throughout the data lifecycle mapped against the legislations of Asia Pacific locations per *The Asia Pacific Privacy Guide, Deloitte-July 2019.*

Location	Definition of personal information/ data		Collection and notice	Usage and disclosure	Data retention and destruction
	Personal	Sensitive			
Australia	✓	✓	✓	✓	✓
Brunei Darussalam	✓	✗	✓	✓	✓
Cambodia	✗	✗	✗	✗	✗
China	✓	✗	✓	✓	✓
Hong Kong	✓	✗	✓	✓	✓
India	✓	✓	✓	✓	✓
Indonesia	✓	✗	✓	✓	✓
Japan	✓	✓	✓	✓	✓
Lao PDR	✓	✗	✓	✓	✓
Malaysia	✓	✓	✓	✓	✓
Mongolia	✓	✗	✓	✓	✗
Myanmar	✗	✗	✗	✗	✗
New Zealand	✓	✗	✓	✓	✓
Papua New Guinea	✗	✗	✗	✗	✗
Republic of the Philippines	✓	✓	✓	✓	✓
Singapore	✓	✗	✓	✓	✓
South Korea	✓	✓	✓	✓	✓
Sri Lanka	✗	✗	✗	✗	✗
Taiwan	✓	✓	✓	✓	✓
Thailand	✓	✓	✓	✓	✓
Vietnam	✓	✗	✓	✓	✗

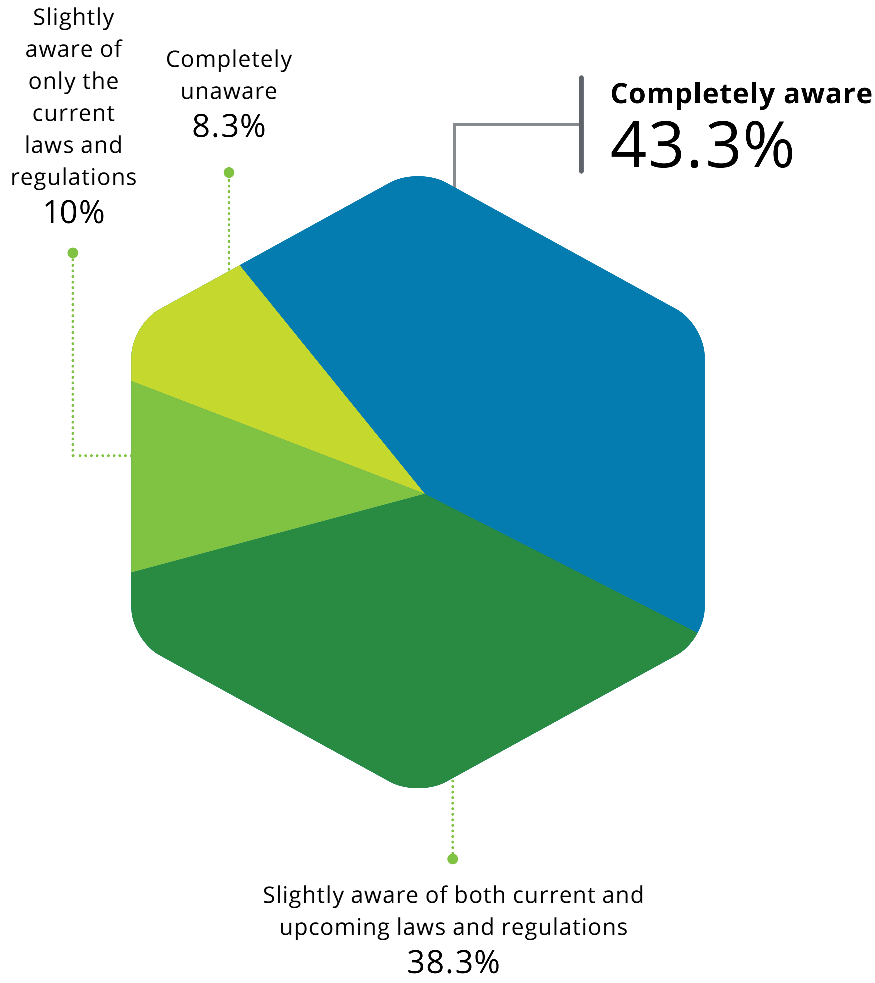
[2] The Asia Pacific Privacy Guide 2019 (https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-unity-diversity-privacy-guide.pdf), Deloitte, July 2019

Evolution of data retention

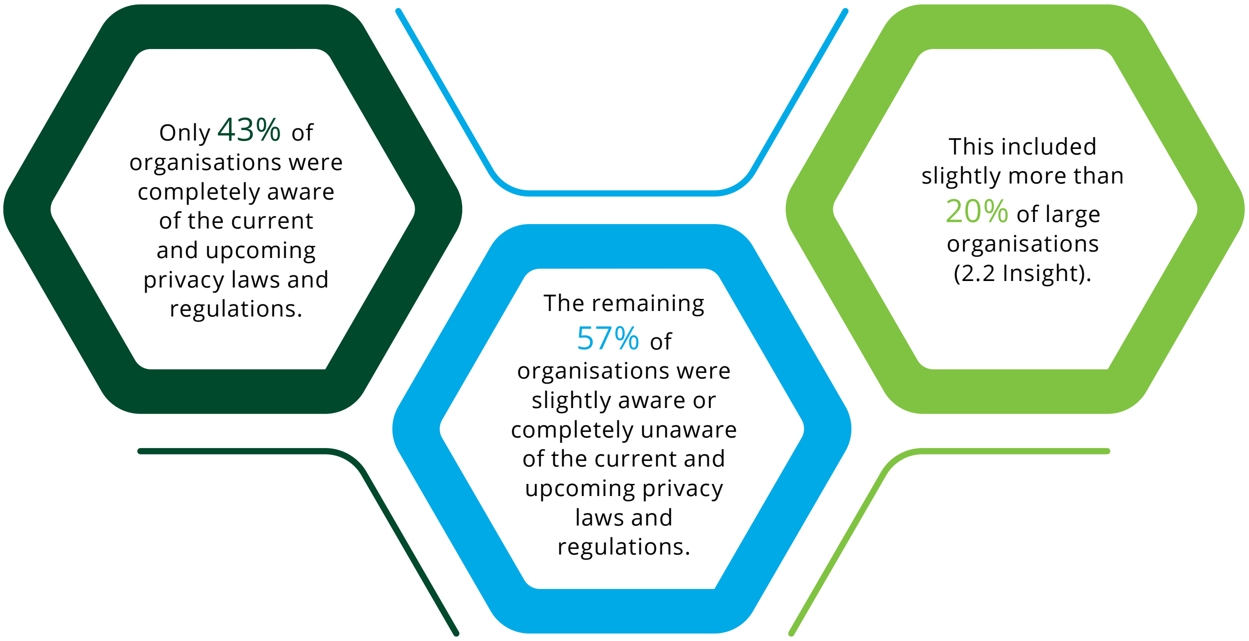
Data retention started out as a practise to maintain records in a systematic manner of labelling and classifying data for easier retrieval when needed. With data getting more complex, the need for good retention practices increased, and privacy laws started to encompass data retention as a requirement. Hence, the need for having different retention periods for different types of data such as personal or sensitive personal data came into existence. In today's digital age, organisations should address both data retention and data disposal rather than ignoring one or the other. They should also define data classification mechanisms, safeguards for protection of personal and sensitive personal data from unauthorised use, modification and disclosure, retention periods by data category, etc. This exercise calls for knowledge of regulation requirements and how to prepare for them.

A lack of knowledge makes organisations more vulnerable to administrative fines or penalties and unintentional data loss. The mere enforcement of a law does not lead to awareness of it.

2.1 Awareness of current and upcoming laws and regulations around data privacy



2.1 Insight



Only 43% of organisations were completely aware of the current and upcoming privacy laws and regulations.

The remaining 57% of organisations were slightly aware or completely unaware of the current and upcoming privacy laws and regulations.

This included slightly more than 20% of large organisations (2.2 Insight).

In the future, organisations may retain data indefinitely to deal with unpredictable situations (where they may require historic data). One of the most important reasons to keep historical data is machine learning (which requires large data sets to improve accuracy), automated profiling of customers for marketing (as long as the customer has provided consent), and other technologies fuelled by data itself.

An overview of the data retention and destruction requirements in GDPR, draft PDPB 2019 and the globally recognised National Institute of Standards and Technology (NIST) 800-88 Media Sanitization Guidelines from the US is as follows:

European General Data Protection Regulation (EU GDPR)

On 25 May 2018, the GDPR came into effect throughout Europe, and provided multiple requirements for any global business that handles data from EU data subjects. The GDPR recognises the 'right to erasure' and extends the longstanding requirement that the Data Protection Directive contained: the data subjects have the right to request that their data be disposed of effectively and responsibly. The GDPR expands this right (and supersedes the Directive) to include data that lives on the internet. Data subjects can also request that they 'be forgotten' from the public view in specific circumstances. While the right to be forgotten has received a lot of media attention, the GDPR also includes important data minimisation requirements that are dangerous to overlook. Data minimisation is defined as the practice of limiting personal data collected to the bare minimum required for its original purpose.[3]

India's draft PDPB, 2019

Post approval by the Union Cabinet, India's draft PDPB, 2019 was introduced in the Lok Sabha (Parliament) on 11 December 2019. As we prepare this survey report, its understood that the bill is under review by Parliamentary Select Committee.

Draft PDPB 2019 is expected to have extensive implications for any global organisation that processes the personal data of Indian residents. Until now, privacy regulations in India, such as the IT Act 2000, Sensitive Personal Data and Information (SPDI) rules, 2011 offered little in terms of data privacy. The new bill is designed with penalties for sharing or processing data without permission and not adhering to appropriate privacy and security safeguards. Fines can be as much as INR 15 crore (approximately US$ 1.9 million as of March 2020), or 4 percent of an organisation's worldwide turnover.

Relevant data retention and erasure requirements from draft PDPB 2019 are as follows:[4]

- Chapter II (4): Data Protection Obligations
  - **Restriction on retention of personal data:** This section discusses data deletion beyond its retention period. The data will only be kept beyond retention periods if there is explicit consent or if there is any obligation under any law.
- Chapter V (20): Rights of Data Principal
  - **Right to be forgotten:** The data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciary related to the data principal where such disclosure has served the purpose and consent has been withdrawn or was made contrary to the provisions of the act.

Data minimisation is another key data management leading practice covered in the regulation (Statement of Objects and Reasons, draft PDPB 2019). The bill states the following: (i) to promote the concepts such as consent framework, purpose limitation, storage limitation, and the data minimisation; (ii) to lay down obligations on entities collecting personal data (data fiduciary) to only collect the data required for a specific purpose and with the express consent of the individual (data principal).

NIST Special Publication 800-88, Rev. 1, 'Guidelines for Media Sanitisation'

NIST 800-88 has introduced a crucial step in data disposal, which is the verification and certification of data sanitisation. Such certification documents the extent or degree of effectiveness of data disposal. A certificate of sanitisation documents the type of sanitisation applied and to what devices. This certificate provides auditable proof of sanitisation to prove compliance with data privacy mandates. It can also increase organisations' trust towards their third-party vendors who perform data sanitisation and contracted vendors that manage data on the organisations' behalf.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[4] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

There are several business benefits of putting an end-to-end erasure policy in place, beyond adhering to existing and upcoming legislations. Some of the benefits include the following:

1. **Reduced attack surface–**More data storage means more points of attack. Hence, retaining unnecessary data brings greater liability, as it can still cause harm if exposed, rendering the organisation liable for brand damage, identity theft, etc.

2. **Security–**The difference between data deletion and erasure is often misunderstood and they are sometimes considered the same. It is important for businesses to understand that if personal, proprietary, or otherwise confidential data is deleted, it is recoverable; if it is erased properly, it is irretrievable.

3. **Cost–**Data storage, both physical and virtual, bundled along with the attached cost of security controls and overhead cost of audit, turns out to be an expensive affair. Being able to erase data securely enables businesses to recycle and reuse storage media without fear of inadvertently placing sensitive data in other's hands. This is a significant advantage to data erasure in comparison to physical destruction of the storage media, which renders it unusable for future use.

Evolution of data disposal

The practice of data disposal started when data was stored only physically (e.g., on paper) and not digitally. Once the digital transformation journey for organisations started, and organisations moved to adopt information technology systems, data destruction of both digital and physical media became essential. Data destruction has seen drastic changes over the years as the volume and complexity of data and data storage has changed with technology advancements. Data destruction covers all the means to render data irretrievable, whether it is in a hard copy or a soft copy, including methods of degaussing, destroying hard drives, etc. However, data destruction does not necessarily include verifying that the data has been destroyed.

Process of data disposal and data sanitisation

In case of digitally stored data, simple deletion of data is not true deletion at all. It simply means removing the index, or pointers, to the data. This data can still be retrieved using software-based data recovery solutions. However, data sanitisation, offers a non-recoverable solution. Whether by physical destruction, cryptographic erasure, or data erasure, data sanitisation deliberately, permanently, and irreversibly removes or destroys the data on a memory device to make it unrecoverable.

As organisations across the globe become more customer centric, it becomes inevitable for them to consider new and upcoming privacy laws and standards and include the relevant data disposal and sanitisation practices for their Global Capability Centers (GCCs) in India. For example, the U.S. NIST defines leading practices to achieve data sanitisation and render data unrecoverable.

Incorporating such practices in GCC will gratify legal obligations, not only locally but also across geographies, giving rise to an integrated approach. Not only do these practices fulfil regulatory requirements, but they also prove to be an effective way to build customer trust and to gain a competitive edge.

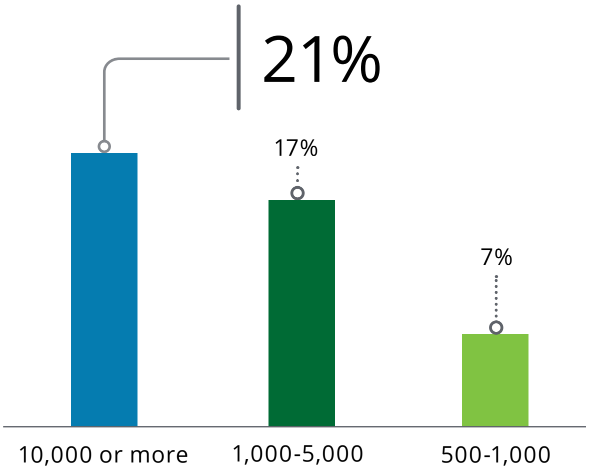
2.2 Insight:

Unawareness of data sanitisation or data erasure increased with organisation size. Large organisations (10,000 or more employees) were significantly more unaware about data sanitisation and erasure practices and requirements than smaller organisations with 500–1,000 employees. It indicates that smaller organisations are better aware of data sanitisation practices and understand the critical risks of maintaining data, which has passed its retention period.

When data does not have to be retained for any added business value or legal purposes, organisations must securely dispose of data. Organisational data is scattered across multiple devices (such as servers, cloud, and virtual machines) and; hence, organisations should create disposal policies around when and how to dispose of data from all devices rather than removing data from specific types of physical assets only (such as desktops or laptops).

Gartner has placed data sanitisation at the beginning of the upward 'Slope of Enlightenment' in three of its reports, the *Hype Cycle for Data Security, 2020*[5]; *Hype Cycle for Privacy, 2020*[6]; and *Hype Cycle for Endpoint Security, 2020*[7]. According to the research, "Growing concerns about data privacy and security, leakage, regulatory compliance, and the ever-expanding capacity of storage media and volume of edge computing and IoT devices make robust data sanitisation a core C-level requirement for all IT organisations." Data protection mandates have increased the awareness of data sanitisation needed amongst government organisations and private enterprises, and many are revisiting their data privacy policies with respect to safe data disposal. Privacy concerns also led to administrative fines and penalties that regulators and courts impose per applicable privacy laws and regulations. While retention is still a critical part of regulatory compliance and business operations, there's a greater need to ensure that retention doesn't turn into hoarding, and that secure data sanitisation is implemented when retention periods are complete.

2.2 Unawareness of data sanitisation or data erasure per size of organisation



[5] Gartner, Hype Cycle for Data Security, 2020, Brian Lowans, 24 July 2020
[6] Gartner, Hype Cycle for Privacy, 2020, Bernard Woo, Bart Willemsen, 23 July 2020
[7] Gartner, Hype Cycle for Endpoint Security, 2020, Dionisio Zumerle, Rob Smith, 15 July 2020

In addition, regulators and courts have imposed fines and penalties for not following data retention, disposal and sanitisation requirements. Some examples are below:

1

On 28 May 2019, the French Data Protection Authority (the CNIL) imposed a €4, 00,000 fine on a real estate company for data security breaches and non-compliance with data retention periods under the GDPR. It was noted that the company kept the personal data of applicants (who did not access the rental) in an active database for a period exceeding the necessary time. This was done to process the allocation of housing, without any intermediate archiving solution in place.

2

On 30 October 2019, the Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA) imposed a fine of €14.5 million on a real estate organisation for not complying with the GDPR. The organisation had used an archiving system for storing the personal data of their tenants, which did not allow deletion of personal data that was no longer necessary. The personal data affected included sensitive data, such as extracts from employment and training contracts, tax data, social security and health insurance data, and bank statements.

3

In 2019, the Data Protection Authority of Niedersachsen fined an organisation €2, 94,000 for 'unnecessarily long' storage and retention of personal data of personnel and 'excessive' collection in the selection process. In some cases, this data dated back many years.

4

In June 2019, the Privacy Commissioner for Personal Data (the PCPD) of Hong Kong issued an enforcement notice against a leading airline company for a data breach concerning personal data of some its customers. This was related to two aspects of the Personal Data (Privacy) Ordinance (the PDPO) Hong Kong:

i. The obligation under Data Protection Principle 4 (DPP 4) to take all practicable steps to ensure that personal data are protected against unauthorised access

ii. The obligation under Data Protection Principle 2(2) (DPP 2) to take all practicable steps to ensure that personal data is kept no longer than necessary for the fulfilment of the purposes for which it has been lawfully collected.

One of the key challenges faced by organisations according to 2018's *DSCI Deloitte GDPR Preparedness Survey report*[8], is to address data subject rights of 'right to erasure' and the 'right to be forgotten'. Additionally, verifying whether personal data had indeed been erased across all stakeholders, i.e., controllers, processors, sub processors, vendors, etc., was challenging. As part of a solution, organisations can use data overwriting software that provides certified proofs of verification of data removal at known locations. These certified proofs are critical for an audit, and must be in place whether performing data sanitisation in-house or via a third-party vendor.

[8] DSCI–Deloitte GDPR Readiness Survey Report (https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-riks-gdpr-preparedness-survey-report-noexp.pdf), July 2018

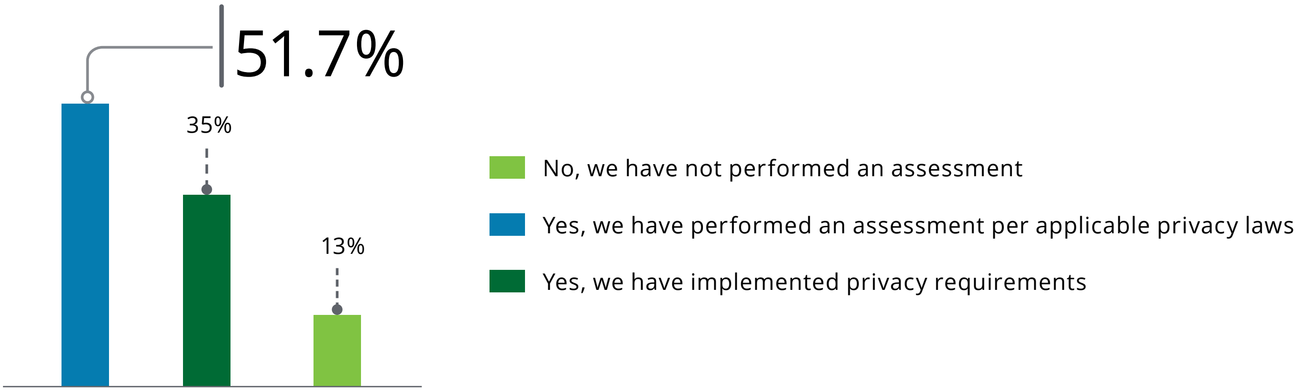
03

Readiness journey of organisations towards data privacy

Journey so far

With the release of privacy regulations around the world, the journey to readiness has been slow but steady.

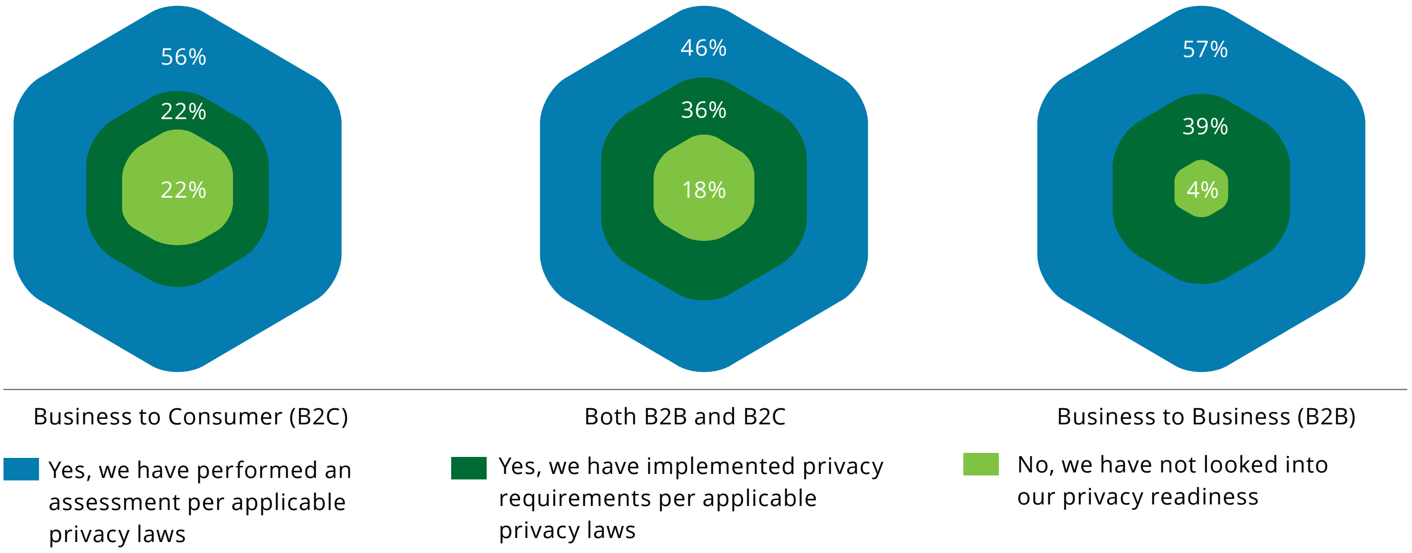
3.1 Readiness journey towards applicable laws and regulations



3.1 Insight:

Nearly eighty-seven percent of the Indian organisations surveyed had begun their journey towards readiness with respect to data privacy regulations. Draft PDPB 2019 brings a renewed focus on privacy laws and regulations, and organisations are becoming more aware of the regulatory requirements to avoid hefty fines and penalties.

3.2 Readiness journey towards privacy (B2B vs. B2C)



3.2 Insight:

As we move from business to consumer-centricity, the number of organisations having initiated their readiness journey towards privacy decreases. In terms of privacy, B2B organisations were more ready compared to B2C organisations. Per the survey, B2C organisations process a high volume of data and hence, need to look into their personal data processing activities at a much deeper level. This process requires a larger monetary as well as time investment, which limits their efforts towards privacy measures.

Due to heavy fines imposed by privacy laws and their implications on the organisation and its reputation, privacy has become a key concern for organisation leaders. Eighty percent of the organisations surveyed had data privacy as a discussion point in their board agenda or audit committee meetings. To drive the privacy programme of the organisation in line with the regulatory requirements, organisations have appointed Data Protection Officers (DPOs) and associated privacy teams.

Data privacy team

The privacy team headed by a DPO manages and delivers the privacy mission and vision statements for the organisation. The privacy strategy is planned by the team for short-term and long-term goals. The responsibilities for each part of the data lifecycle management are defined and assigned to the team.

The final steps of the data lifecycle, i.e., data retention and disposal, require knowledge of technologies and processes for storing, archiving, and destroying data. The wide range of knowledge and skills involved mean that data retention must be an organisation-wide exercise, with participation by legal and compliance experts, lines of business management, and IT and information security staff. Third parties can also play an important role. If the team does not have adequate knowledge and/or resources, third parties may be involved contractually for the data sanitisation process.

The data privacy team should include core members from the following, but not limited to:

1 Legal

2 Internal audit

3 Compliance and risk management

4 Procurement

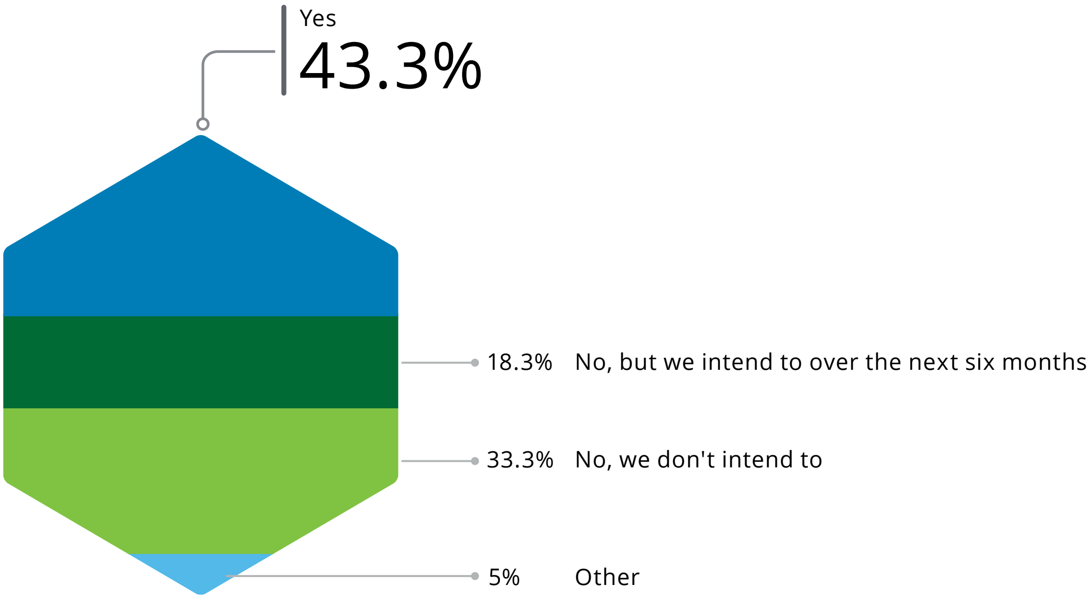
5 Human resources

6 Cybersecurity and information security

7 Business functions

8 Information technology

3.3 Appointment of a DPO



The GDPR requires organisations to appoint a DPO and the Indian draft PDPB 2019 mentions the requirement for significant data fiduciaries to appoint a DPO. The DPO is primarily responsible for dedicatedly managing the data privacy processes in an organisation to maintain its privacy posture.

3.3 Insight:

Only 43 percent of survey respondents had appointed a DPO. Draft PDPB 2019 has a fine of 2 percent of global turnover or INR 5 crore, whichever is higher, for any data fiduciary not appointing a DPO.

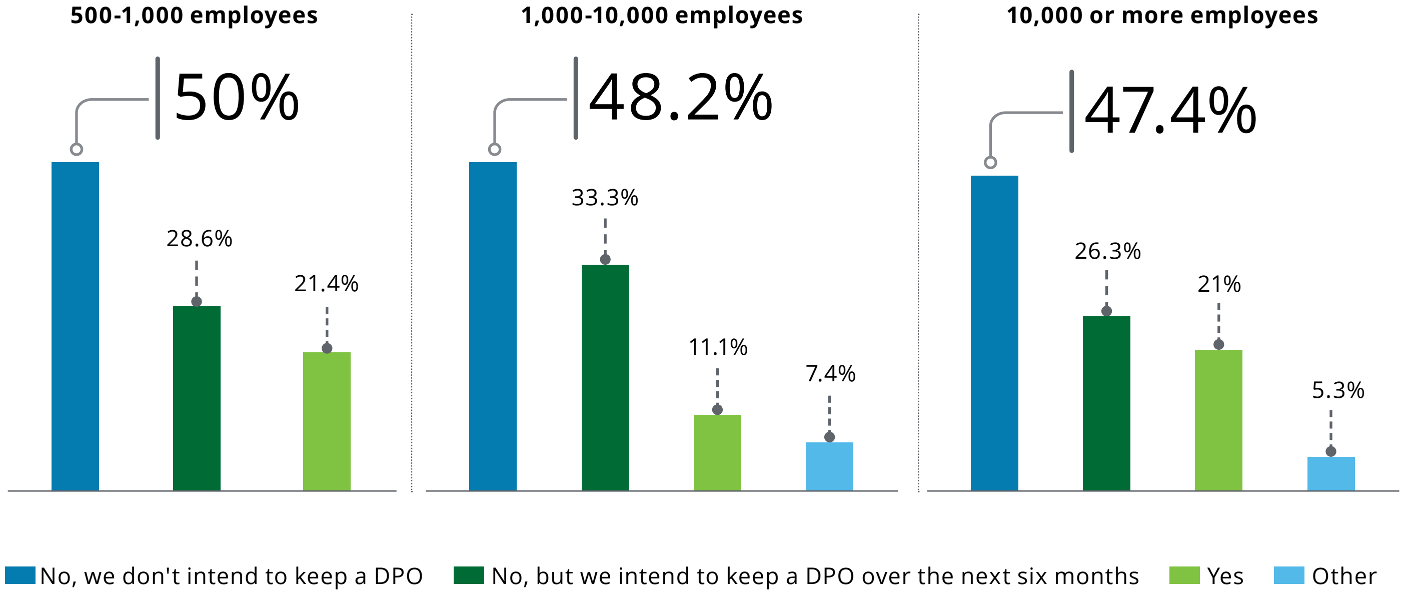
Due to regulatory reasons, the demand for the DPO is increasing substantially and more and more organisations require this position. Per an IAPP article published after the release of GDPR[9], it was estimated that as many as 75,000 DPO positions would be created in response to the GDPR around the globe. With India's draft PDPB 2019 also expecting a similar requirement, it would be safe to assume that the demand for DPOs will increase.

Eighteen percent of organisations intended to appoint a DPO in the next six months. In the absence of a DPO or a structured privacy programme, organisations often experience lapses during the collection of personal data and sensitive personal data. Hence, due to mishandling of data there is a higher risk of breach and penalties. Therefore, DPO appointment is recommended.

3.4 Insight:

Large organisations (10,000 or more employees) tend to have a DPO (or at least intend to have one soon) as compared to small and medium businesses (500–1,000 employees).

3.4 DPO appointment vs. size of organisation



[9] Study: GDPR's global reach to require at least 75,000 DPOs worldwide (https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/)

04

Focus on data retention and disposal

Globally, privacy laws are demanding attention from enterprise leaders for timely readiness and adherence. To comply with the legislations in an exhaustive manner, different roles and responsibilities should be assigned to the privacy team to map and manage the data lifecycle.

Data lifecycle management is the process of managing data throughout its lifecycle from collection to destruction. During its lifecycle, data crosses various applications, systems, media, and databases. The lifecycle typically includes phases such as collection, use, transfer, storage, retention, and destruction. The industry practices at each phase vary per the framework established by the organisation. Following are the different stages of a data lifecycle:

1 **Create–**New data is generated or acquired, or the existing data is altered or updated, which includes any data or content element.

2 **Store–**The digital data is committed/stored to some sort of storage repository (such as a laptop, mobile device, server, or cloud), and typically occurs nearly simultaneously with creation. Threats such as cyber-attacks and malware make it necessary to move towards an ecosystem that protects an individual's privacy. In addition, organisations should be aware of when to collect and when to dispose off all digital or physical data collected to mitigate harm from such threats and attacks.

3 **Use–**Data is viewed, processed, or otherwise used in some sort of activity.

4 **Share–**Data is made accessible to others, such as between users, both internally and externally, including customers and partners.

5 **Archive–**The data leaves the 'active' state and migrates to long-term storage systems for retention.

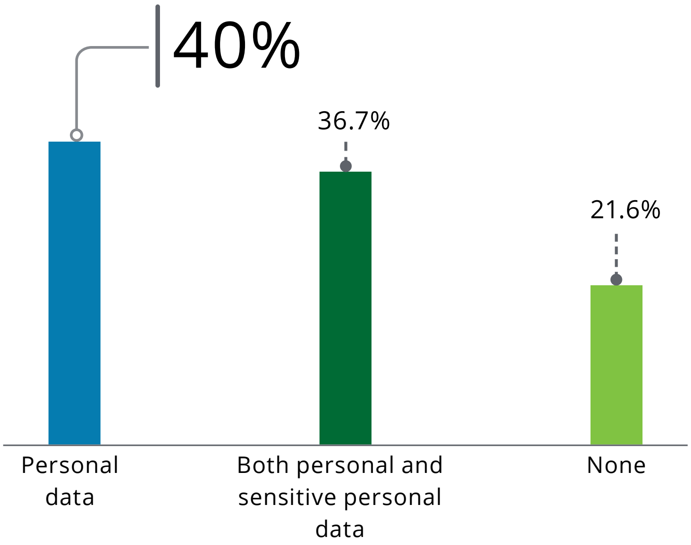
6 **Dispose–**Data sanitisation is performed to make the data permanently unrecoverable through physical or digital means (e.g., physical destruction, cryptographic erasure, or data erasure).

4.1 Insight:

Three out of four organisations collected either personal data or sensitive personal data. Such collection makes it an obligation for organisations to comply with data privacy laws and regulations.

Per the survey, more organisations preferred to manage their personal and sensitive data on their own premises, with the public cloud being the next most popular choice. This may be due to the cost effectiveness of various cloud models. A large number of organisations prefer in-house data centres (on premise) as it gives them greater control on data and related processing activities. It also indicates that organisations recognise the risk and are apprehensive in sharing data with vendors and third parties.

4.1 Type of data collected by organisations



Data retention

Data retention is the practice of storing files or documents for a specific time or indefinitely, due to compliance or business-related reasons.

Need for a data retention policy

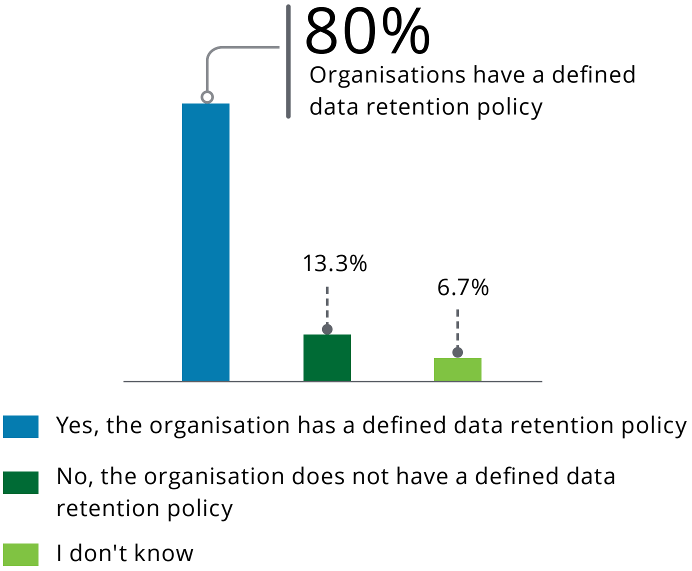
Organisations need to create policies and processes that handle documents and files appropriately, as they migrate across lifestyle stages. These documents raise some key questions: When these files reach the end of required retention periods, should we retain longer or erase them immediately? For sensitive documents with no statutory retention period, how long should we retain these and when should we erase them? How should the organisation handle requests from third parties, such as customers, to delete personal data?

4.2 Insight:

One out of five organisations either did not have a data retention policy or were not aware of whether they had one. To comply with data privacy regulations and laws, every stage of the data lifecycle within the organisation should be analysed. Organisational leaders need to define, communicate, and circulate defined data retention policies to interested stakeholders. However, for organisations that do have a retention policy, the retention practices can only be verified after privacy audits produce certificates as proof of destruction.

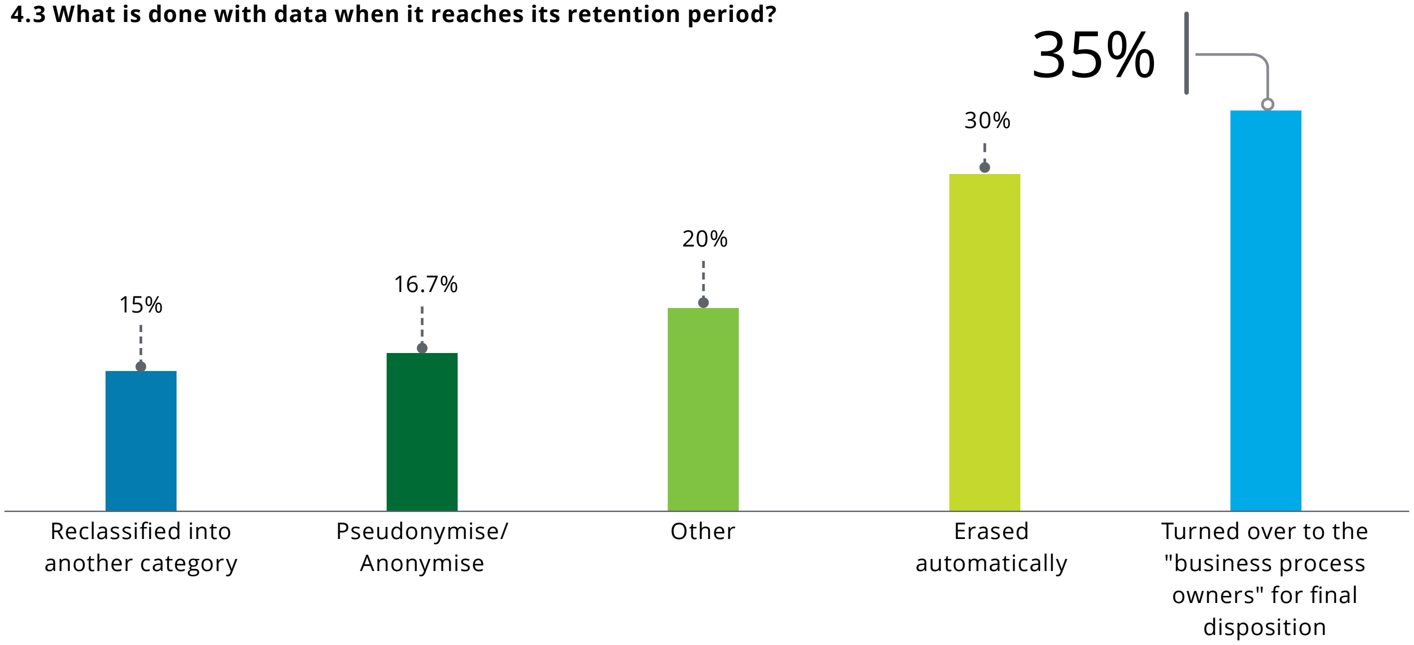
In our survey, 84 percent of large organisations (with more than 10,000 employees) had a defined data retention policy as compared to 57 percent of smaller organisations (with 500–1,000 employees). This aligns with findings that nearly all large organisations collect personal or sensitive data or both (4.1 Insight), much of which would be subject to data retention and destruction requirements. As a drawback, much (42 percent) of large organisation data destruction is handled manually (4.9 Insight), which can be inefficient and prone to error. It is also evident that larger organisations, despite having defined retention policies, may not have the right technology to execute on those policies as far as data sanitisation is concerned. With the increase in size of organisation, there is better documentation of privacy policies such as data retention policies.

4.2 Data retention policies



Information security is one of the major requirements in a data retention policy. From the perspective of information security, data that has been erased can't be stolen and sold by hackers and can't be used against the organisation by anyone else that may be hostile to it. The possible business value of storing data indefinitely must be weighed against the risk of losing control over it.

4.3 What is done with data when it reaches its retention period?



4.3 Insight:

Although organisations have reported the existence of a data retention policy, only one out of three respondents provided data to the business process owners for final disposition. Data is seldom reclassified or anonymised per current practices. Organisations may not be aware of techniques to use anonymised/ pseudonimysed data in an effective manner. Only 30 percent of the organisations were adopting automated erasure techniques for data on completion of the retention period.

Data disposal

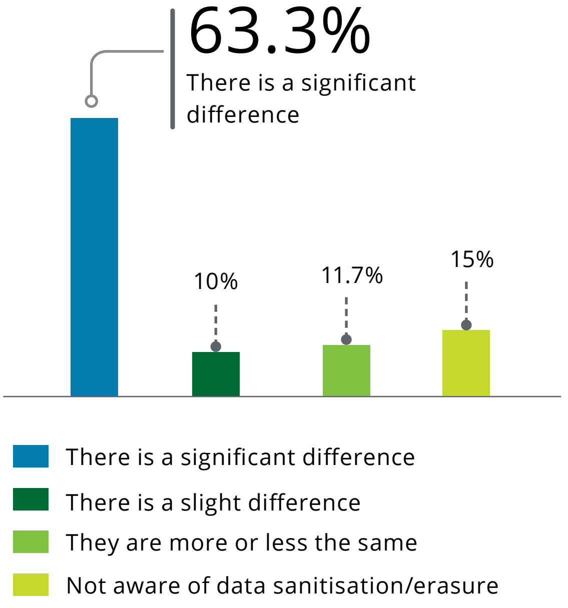
We've previously established that data deletion is ineffective in protecting data. Another improper method of protecting end-of-life data is drive/device formatting.

The key differentiating feature in formatting (also referred to as low-level format, deep format, or full format) is that there is no way to confirm that the data is gone. The processes of verification and certification are key to achieving data sanitisation for security and auditing purposes.

4.4 Insight:

One out of three organisations indicate no significant difference between sanitisation/erasure and formatting. Such organisations are not able to exploit the value of adopting techniques related to data sanitisation and data erasure. There are methods that can help achieve compliance requirements and save cost on technology refresh.

4.4 Awareness of practices related to data sanitisation/data erasure and formatting



According to Blancco's 2019 research study, *Privacy for Sale: Data Security Risks in the Second-Hand IT Asset Marketplace,*[10] more than 15 percent of second-hand drives purchased from an online retailer contained leftover data from the previous users. Sellers also reported that attempts were made to destroy data in those drives.

This leads us to the options available to organisations for removal of data.

4.5 Insight:

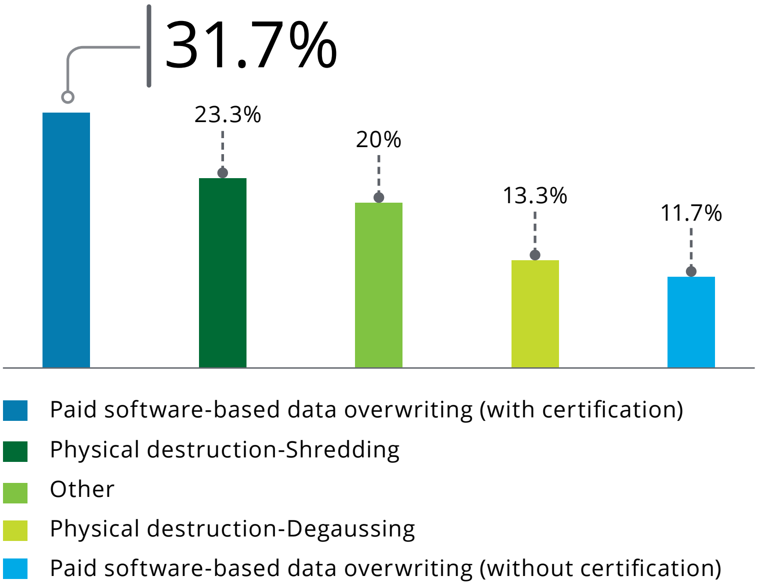
Only 32 percent of organisations produced certification of data removal from solid-state drives at end-of-life. Without proper verified proofs, organisations cannot confirm to data protection authorities that their data has been irreversibly removed from their system. This may arise due to lack of awareness of data sanitisation and its requirements.

This indicates that only 32 percent of organisations are prepared for and may have conducted audits of processing activities with respect to end-of-life of personal data. Most organisations do not understand the need of maintaining data destruction proof. While data may be destroyed, they are not able to demonstrate privacy compliance. In addition, more than a third rely on traditional methods of shredding and degaussing. SSDs are particularly vulnerable to improper shredding as shred size must be much smaller than required for magnetic disk drives. Worryingly, 13 percent of respondents indicated that they degauss their SSDs—a method that is ineffective against solid-state drives and should only be applied to magnetic media. This shows a critical misunderstanding of what it takes to destroy data on SSDs.

Data erasure

Data erasure is a method of software-based overwriting that destroys all electronic data residing on a drive. Unlike degaussing or physical destruction, which render the drive unusable, data erasure removes all data while leaving the drive operable, preserving assets and the environment. It also verifies and certifies that data has been rendered unrecoverable. It allows for remarketing and value return, but not at the risk of data breach.

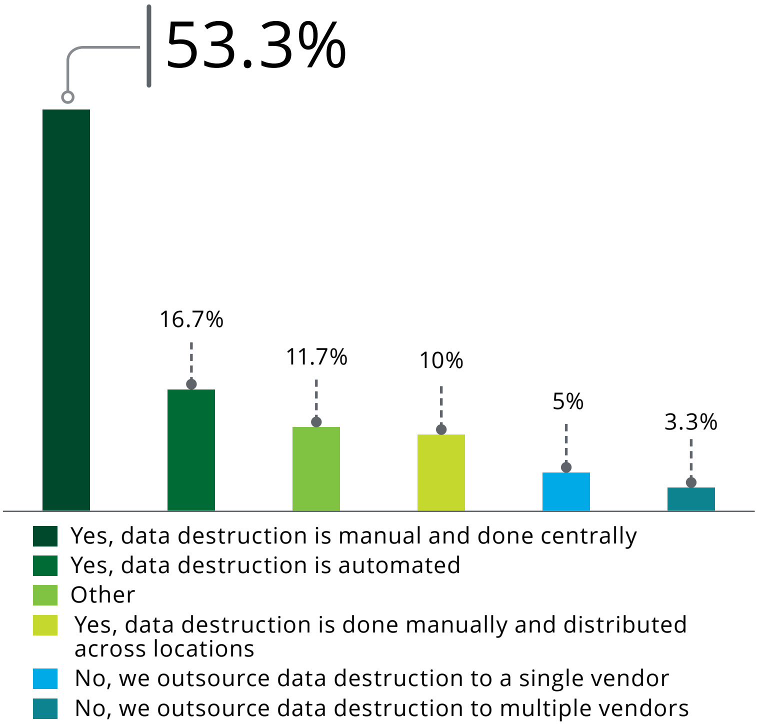
4.5 Removal of data from solid-state-drives (SSDs) at end-of-life



4.6 Insight:

Sixty-three percent of the organisations surveyed had a manual data destruction process. With increased human intervention, there is a higher chance for errors.

4.6 Data destruction practices of organisations



[10] Privacy for Sale: Data Security Risks in the Second-Hand IT Asset Marketplace (www.blancco.com/resources/rs-privacy-for-sale-data-security-risks-in-the-second-hand-it-asset-marketplace/), Blancco Technology Group, 25 Apr 2019

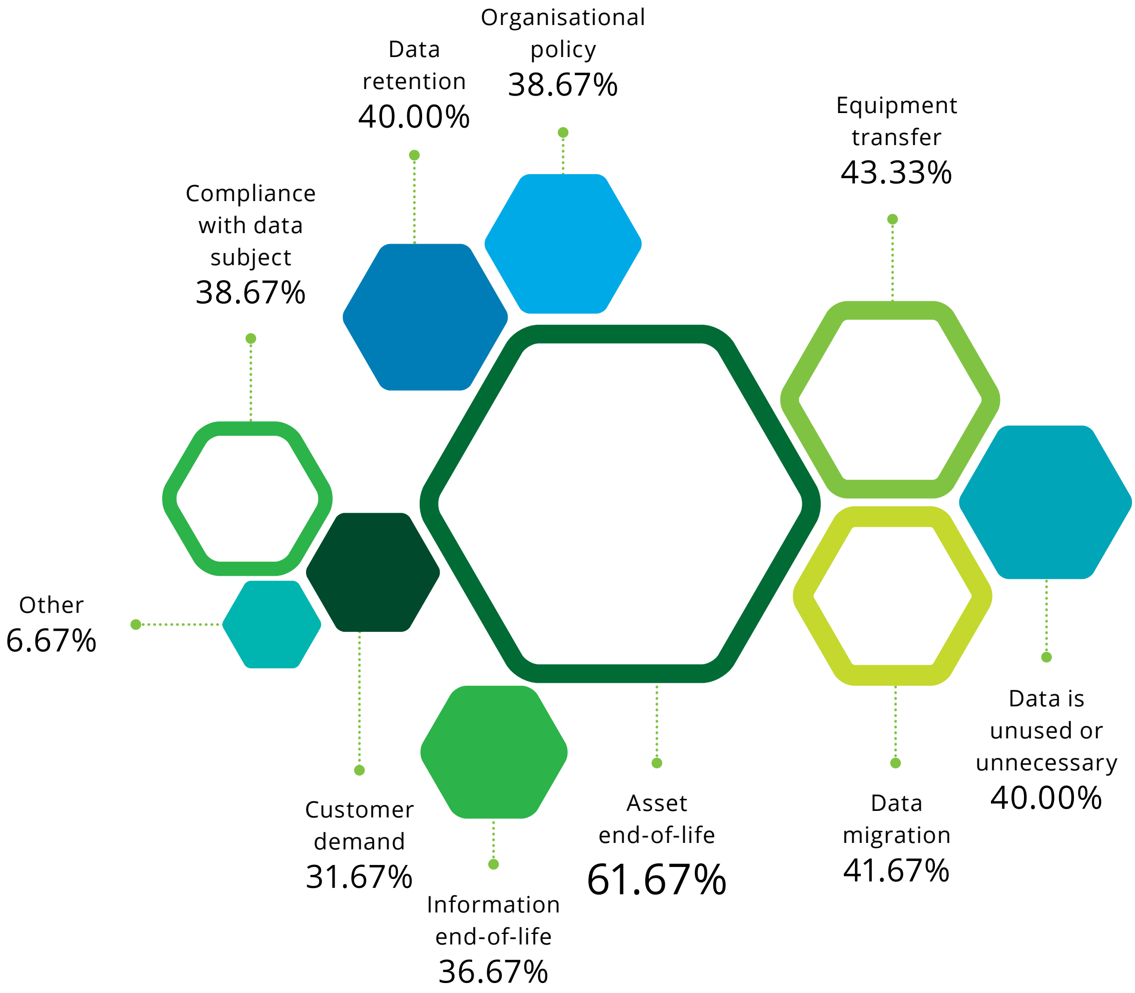
As a leading practice, organisations should automate the data destruction process and ensure proof of sanitisation. Most of the organisations have not outsourced the end-of-life stage as they consider data destruction as a critical process. Data intended to be destroyed may not actually be destroyed and continue to be retained, accidental copies may be neglected, uniformity of destruction across regions may vary and there is no effective way of monitoring the activities.

Risks of retaining more data than required

Ignoring the mandate to erase or otherwise remove unnecessary data can leave organisations with data that can be:

1. Hacked
2. Vulnerable to malware attack
3. Costly during discovery and breach recovery

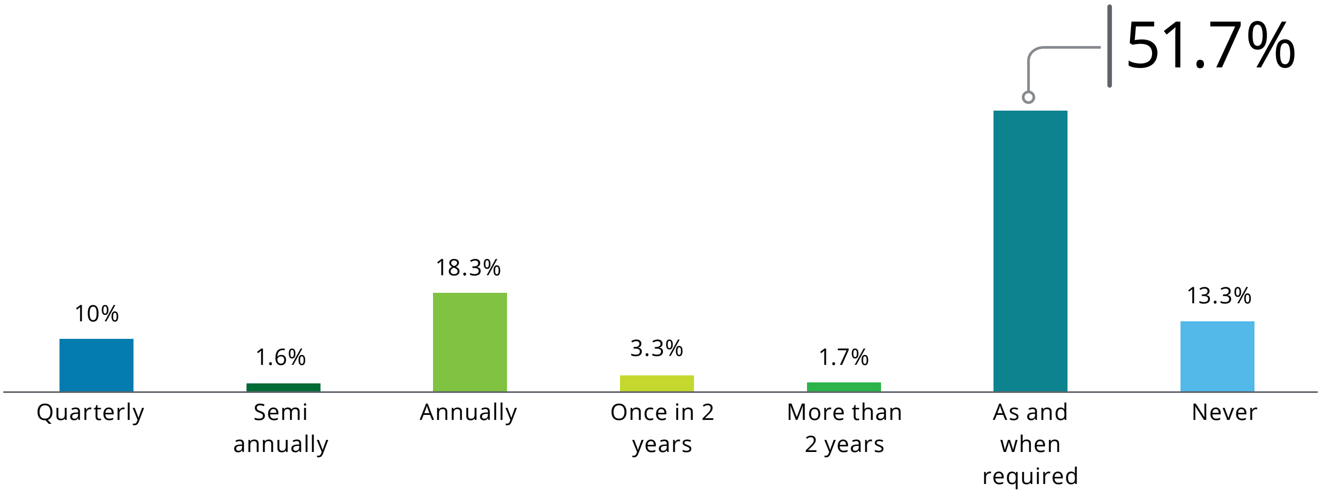
4.7 Reasons for performing data sanitisation



4.7 Insight:

Most of the organisations (62 percent) performed data sanitisation due to asset end-of-life, followed by equipment transfer (43 percent), and data migration (42 percent). Automated methods of data sanitisation can expedite this process. When performing data sanitisation for reason such as asset end-of-life or data migration, a large number of devices and servers will require data sanitisation. This can be time consuming and prone to error without automated solutions in place.

4.8 Frequency of performing data destruction



4.8 Insight:

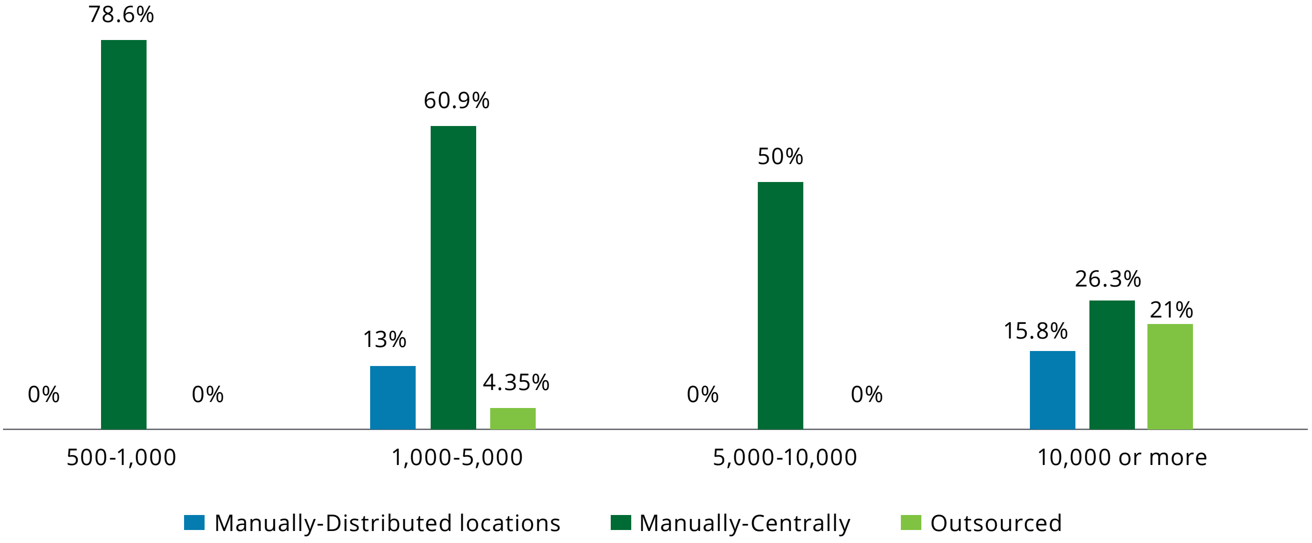
- Approximately half of the organisations did not perform data destruction in a periodic manner, instead perform data destruction as and when required.
- Moreover, 20 percent of the small organisations (up to 5,000 employees) never performed data destruction.

  Data destruction in live environments on a bi-weekly basis is a good practice and is a proactive approach towards complying with regulations and laws. This can be achieved by automating data destruction practices. Sanitising data assets as soon as possible during the decommissioning process also protects drives and devices against data loss or theft. It was seen that with increase in size of organisation, there is more adherence to data destruction per retention policy.

4.9 Insight:

- With the increase in size of organisations, manual data destruction such as shredding, degaussing etc., were distributed geographically and outsourced more often.
- One-fifth of large organisations (10,000 or more) that responded to this survey outsourced their data destruction process.

4.9 Organisations performing manual data destruction



- Forty percent of large organisations (10,000 or more) that responded to this survey manually performed data destruction.
- Also with increase in size, the organisation tries to either outsource or adopt methods such as shredding, degaussing, etc., to support processes distributed geographically.

Major challenges involved with the process of data destruction

Due to increasing association with vendors for various business processes, it becomes difficult for organisations to monitor their practices in compliance with all data lifecycle stages. The most difficult stage to monitor is the last or end-of-life stage of data. Controllers do not have consolidated visibilities into their vendor's data destruction processes, which make it difficult for organisations to ensure and prove compliance with data sanitisation obligations.

4.10 Insight:

The majority (58 percent) of the organisations surveyed did not have any visibility into their vendors' data destruction processes. Hence, there is an uncertainty about the effectiveness of data destruction practices being used by third-party vendors. While organisations are starting to hire vendors to manage the destruction of data in a structured and automated manner, they are not completely aware of the process followed by the vendors. This is because the organisations do not possess the knowledge of the tools and technologies for data destruction. Hence, organisations rely on the subject matter expert, experience of the vendors, and the contractual obligation to get the job done rather than checking the actual processes followed.

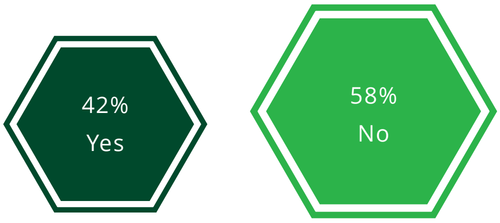
4.11 Insight:

Large organisations (43 percent) had more visibility over third-party vendor's data destruction process compared to SMEs that do not have any kind of visibility. With increase in size of organisation there is a higher visibility into the vendor's data destruction techniques and hence, the process adopted by the vendor can be verified.

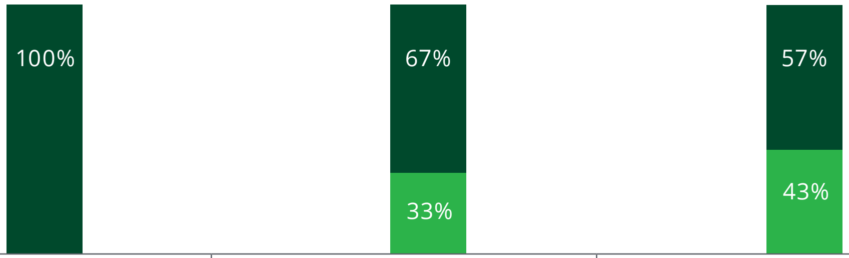
4.12 Insight:

B2B organisations had more visibility over their third-party vendor's data destruction process compared to B2C organisations.

4.10 Visibility into vendors' data destruction process



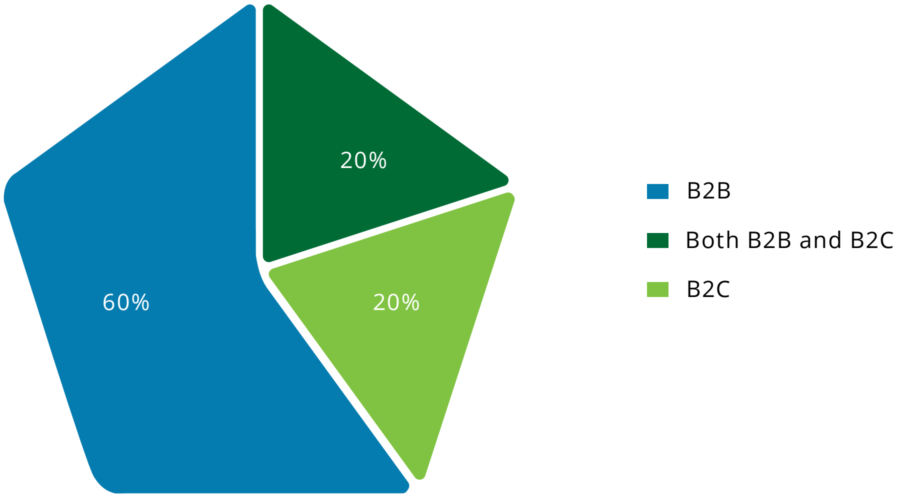
4.11 Do you have visibility into your vendor's data destruction process?



Between 500 and 1,000	Between 1,000 and 5,000	10,000 or more
100.00%	66.67%	57.14%
0.00%	33.33%	42.86%

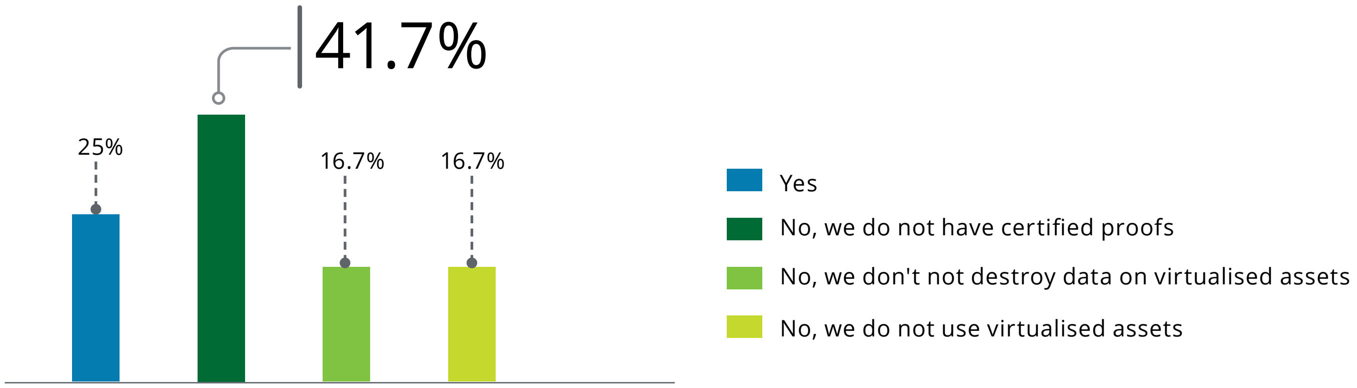
■ No 🟩 Yes

4.12 Visibility into vendor's data destruction process



One of the major challenges to erase a given data set or record is applying changes or removal of data from various backup copies. However, some data storage sites may be offline, inaccessible, or stored at a third-party site during the erasure operation. Therefore, the challenge is to ensure 'eventual' erasure of all copies of the data, including copies used by vendors and contractors. In this case, third parties must be able to produce certified proof that the data has been sanitised. That process should be agreed upon during the contracting, procurement stage before work has begun, and data is shared. Software-based data overwriting solutions should erase according to specified standards and be verified with a digitally signed certificate of erasure.

4.13 Certified proofs of data destruction for virtualised assets



4.13 Insight:

Only 25 percent of the survey respondents had certified proofs of data destruction for virtualised assets. Data destruction without verification and certification is not an adequate practice. Compliance with data privacy-related regulations typically requires organisations to present certified proofs of data sanitisation and the standards used.

Organisations have started receiving data destruction requests from data subjects after the enforcement of GDPR. They face the challenge of taking swift action for the request received with a short turnaround time. The organisations should have a framework in place to achieve the desired result.

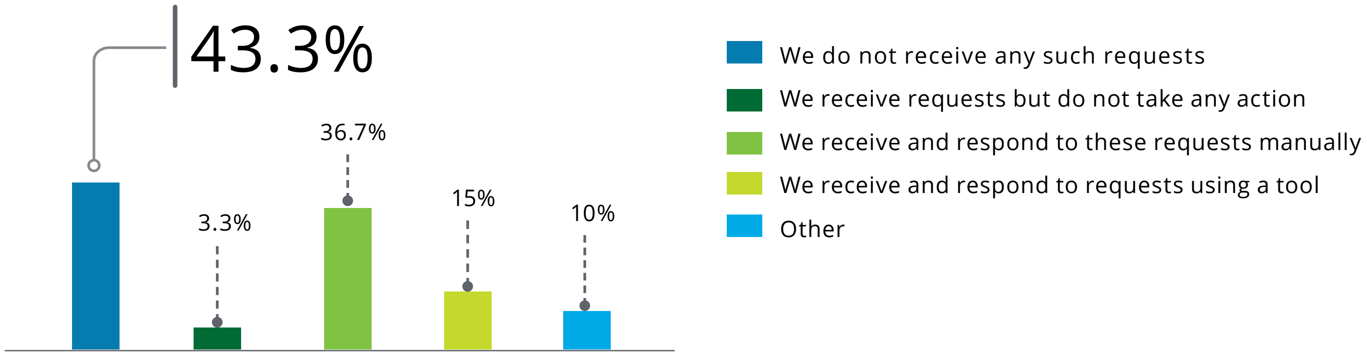
4.14 Insight:

Only 52 percent of the organisations received and addressed data destruction requests from data subjects. Most of the data privacy laws and regulations make it a requirement to respond to data subject requests for deletion of their data and the organisations must adhere to such requests within the mandated timeframe. Forty-three percent of the organisations do not receive Data Subject Rights requests and do not consider themselves as data controllers under GDPR. In the absence of the Indian privacy law, there are no Data Subjects' Rights requests provided to India data principals.

For organisations that do not have a detailed view of the data lifecycle, data destruction requests can be a cumbersome exercise. Such organisations would not have a view of the number of places, data lineage, and which stakeholders maintain a copy of the data.

For organisations that use a certification mechanism for destruction of data (in cases where a data subject request for deletion of data is received), the certificate assures the user of the deletion of data.

4.14 Addressing data destruction requests



05
Conclusive remarks

With the growing volumes of data being processed by organisations across the world, the journey towards achieving readiness towards data retention and disposal is filled with obstacles and constraints. Organisations must be made aware through education about legal and regulatory requirements and leading practices. Organisations must also consider that data is an asset as long as it has an associated purpose. Once the purpose is fulfilled, continuing to hold the data may lead to data becoming a liability, thereby making data sanitisation an even more important part of the data lifecycle. This journey can be simplified if the organisations understand the data lifecycle and requirements for data retention and disposal.

Survey findings indicated lower levels of awareness and readiness amongst larger organisations and B2C organisations. Such organisations, compared to smaller or B2B organisations lack visibility over third-party vendor's data destruction methods and are slow in establishing retention periods for personal and sensitive personal data.

Today, organisations are expected to identify end-of-life data and timelines for data sanitisation.

The major challenges that came out through this survey are the following:

1) The majority of organisations do not have consolidated visibilities into their vendors' data destruction processes, which makes it difficult to comply with relevant regulations and laws.
2) Organisations struggle with removing all copies of a data record (so that no replicas of that data remain).
3) A significant number of organisations handle data subject requests manually and hence may not be able to respond to data subject requests within the stipulated time as manual processes are time consuming.
4) Twenty percent of organisations do not have definite retention policies. The organisation must build a strong privacy team with roles and responsibilities that are defined and segregated. A strong demand for appointing a DPO within the organisation is mandatory, according to the upcoming laws and regulations. Along with these practices, a data retention policy and programme also provides the right direction for an organisation to comply with relevant regulations and protect sensitive data that has reached end-of-life.

Once organisations perform data retention activities, they will be able to identify what data needs to be disposed off. From there, organisations can improve their data protection and compliance posture by:

1) Improving awareness and education on data sanitisation requirements for verification and certification (as standards such as NIST 800-88 require)
2) Improving insight into vendor data and device destruction practices so that organisations can ensure compliance with changes in laws and regulations
3) Incorporating onsite erasure when possible, and enabling greater transparency into the data disposal process and additional security and immediacy in erasing drives without the need to transport elsewhere
4) Adopting processes that enable live erasure of files and folders in active environments to ensure a comprehensive methodology in achieving data retention and data disposal regulation compliance

Connect with us

Rohit Mahajan
President - Risk Advisory
Deloitte Touché Tohmatsu India LLP
rmahajan@deloitte.com

Manish Sehgal
Partner, Risk Advisory
Deloitte Touché Tohmatsu India LLP
masehgal@deloitte.com

Gaurav Shukla
Partner, Risk Advisory
Deloitte Touché Tohmatsu India LLP
shuklagaurav@deloitte.com

Liz Adams
Global Marketing Director, Blancco
liz.adams@blancco.com

Anurag Nalawade
Country Manager, India, Blancco
anurag.nalawade@blancco.com

Contributors

The Data Destruction Survey Report is the result of the efforts of the Deloitte's Risk Advisory practice and Blancco's project team. The report has been shaped by the responses and experience of practitioners from 60 organisations across a variety of sectors.

Deloitte
Kartikeya Raman
Ambika Bahadur
Aditya Sharma
Rati Acharya
Aneesha Sharma
Ankita Chawla

Blancco
Anurag Nalawade
Vivian Cullipher

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.