How Blancco Helps Organizations Comply with India's Personal Data Protection Bill

In 2018, the Justice Srikrishna Committee of India released its much-awaited draft Personal Data Protection Bill. This bill is set to be finalized in late 2019 or early 2020, and when it does, it will have far-reaching applications for any global company that processes personal data for India's residents. Until now, privacy regulations in India, such as the Sensitive Personal Data and Information, 2011, offered little in the way of data protection. The new bill is modeled after Europe's General Data Protection Regulation, with penalties for sharing or processing data without permission. Fines can be as much as ₹15 crore, or 4 percent of a company's total worldwide turnover.

How Does the Bill Define 'Data Processing'?

The term "processing" is referred to throughout the bill. Therefore, before we go into more specifics, let's look at how the Committee defines this term. The bill states: "'**Processing**' in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organi[z]ation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction."

What Does Data Processing Mean Regarding Data Sanitization?

As stated in the definition above, data processing includes data erasure or destruction. A few points must be considered in this:

1. **Always Sanitize** – Data removal should be carried out in a way that data cannot be recovered through any forensic means. (Thus, formatting, deleting and other methods that don't achieve full data sanitization are insufficient).

2. **Always Verify** – Perform an automated read operation to confirm data erasure/destruction. Many data security and privacy regulations mandate verification as a part of the data sanitization process.

3. **Always Certify** – It's best practice (see NIST SP 800-88 Rev. 1) to use data erasure methods that automatically generate certified, tamper-proof erasure reports for auditing purposes.

Personal Data Protection Bill Highlights

RELEVANT PRINCIPLES FROM THE BILL	HOW BLANCCO HELPS
Principle 2. Storage Limitation **CHAPTER II (5)- DATA PROTECTION OBLIGATIONS -** 10. Data storage limitation. — (1) The data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed. (2) Notwithstanding sub-section (1), personal data may be retained for a longer period of time if such retention is explicitly mandated, or necessary to comply with any obligation, under a law. (3) The data fiduciary must undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession. (4) Where it is not necessary for personal data to be retained by the data fiduciary under subsections (1) and (2), then such personal data must be deleted in a manner as may be specified. 11. Accountability— (1) The data fiduciary shall be responsible for complying with all obligations set out in this Act in respect of any processing undertaken by it or on its behalf. (2) The data fiduciary should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this.	When data does not have to be retained for added business value or retention purposes, organizations must securely dispose of it. As organizational data is scattered across multiple types of devices, organizations should focus their disposal policies around when and how to dispose of data from all IT devices, as opposed to removing data from specific types of assets such as desktops or laptops. Blancco data erasure software helps organizations remove data from end-of-life IT assets and active environments when it has reached the end of its retention date or usefulness. Additionally, Blancco File Eraser allows organizations to set up time-based triggers for data erasure in active environments to further satisfy such requirements. To achieve accountability, Blancco Management Console (BMC) provides the ability to create and manage detailed audit logs with dates and timestamps to prove compliance. Additionally, with BMC, the data fiduciary can have separate user groups within the Console for all the different entities managing company data as it pertains to erasure. This will enable the fiduciary to ensure erasure processes are being followed by other data processing entities.
CHAPTER VI DATA PRINCIPAL RIGHTS 27. Right to Be Forgotten. — (1) 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— (a) has served the purpose for which it was made or is no longer necessary; (b) was made on the basis of consent under section 12 and such consent has since been withdrawn; or (c) was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.	As the data principal has the right to be forgotten, all data with regard to the principal must be erased when required. As this data may be scattered across devices, it is important to have erasure solutions that cater to all types of devices. With this in perspective, the following Blancco solutions will be useful. • **Blancco File Eraser** – If you have identified personally identifiable information (PII) on the file level (e.g., a copy of a customer database or a file structure with individual files and folders), Blancco File can target and erase files on computers and servers. The solution is available on both UNIX and Windows operating systems. • **Blancco Drive Eraser** – When you are re-deploying or decommissioning entire drive-based systems containing personal data, Blancco Drive Eraser increases endpoint security by erasing all data securely on enterprise laptops and desktops, as well as servers, storage systems and loose drives. • **Blancco Mobile Diagnostics & Erasure** – Once you have identified personally identifiable information on mobile devices or tablets, Blancco Mobile Diagnostics & Erasure can target and erase data on any device that's iOS or Android-based, using factory reset or other more advanced erasure methods. • **Blancco LUN / Virtual Machine Eraser** – If you have stored PII temporarily on virtual volumes or in virtual machines, on premise or in the cloud, Blancco Virtual Machine Eraser and/or Blancco LUN Eraser can securely target and erase this data.

RELEVANT PRINCIPLES FROM THE BILL	HOW BLANCCO HELPS
CHAPTER VII TRANSPARENCY AND ACCOUNTABILITY MEASURES 34. Record-Keeping. — (1) The data fiduciary shall maintain accurate and up-to-date records of the following— (a) important operations in the data life-cycle including collection, transfers, and **erasure**[1] of personal data to demonstrate compliance as required under section 11. 35. Data Audits. — (1) The data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act. (2) The data auditor will evaluate the compliance of the data fiduciary with the provisions of this Act. 61. Codes of Practice. — (6) Authority may issue codes of practice in respect of the following matters [...] (n) methods of destruction, deletion, or **erasure**[1] of personal data where required under this Act.	To maintain up-to-date records, every erasure (for drives, files, folders, VMs, etc.) should generate an erasure report. Also, this erasure report should contain the erasure algorithm and verification percentage as specified by regulations such as NIST SP 800-88 Rev 1. Once such an erasure report is generated, it is important that the following is achieved: 1. Automatic archival of erasure records: Blancco offers the ability to automatically archive data erasure records so that there are readily available to prove compliance. 2. Easy searchability: once archived, Blancco Management Console organizes data erasure records for easy searchability. It also provides: a. Extended search through auto-captured parameters, allowing users to search by hardware attributes b. Search through organization-specific custom fields like department name, location, etc. By implementing data erasure solutions across the full data lifecycle, organizations can meet and exceed data sanitization best practices outlined here and in other relevant guidelines. An efficient data erasure process can be set up across all live environments and end-of-life assets, with full visibility of the data erasure process through Blancco Management Console, across various teams or locations. This provides transparency and accountability across the full data erasure process. With an erasure report for each asset, file, folder, etc. that's erased, Blancco customers receive a Certificate of Erasure for auditing purposes. Blancco also provides an option to allow auditors to log in to the customer's Blancco Management Console through an auditor-specific role. This makes it easy to prove compliance. Blancco's data erasure solutions have been certified, recommended and approved by 15+ global organizations. Our data sanitization experts can help global organizations set up a proper data sanitization process across all data and data-bearing assets to fulfil this and any other erasure requirements.

Privacy by Design is another key data management best practice covered in the regulation (Section 29). The Privacy by Design approach focuses on minimizing the collection of personal data, erasing personal data that's no longer necessary, restricting access to sensitive data and protecting data throughout its entire lifecycle.

In other words, Privacy by Design is about proactively embedding privacy into the design and operation of IT systems, networked infrastructure and business practices from the start. By focusing on erasing data throughout the full data lifecycle and building data erasure practices into existing data management policies and processes from the beginning, organizations are well on their way to achieving this best practice.

Continued...

[1] *Our emphasis*

Data sanitization should be considered through a holistic perspective in which all types of devices and data are considered. An efficient process should be set up for maintaining audit logs for every erasure performed. When possible, the data erasure process should also be integrated with existing systems like Active Directory, IT asset management systems, etc.

Why Blancco?

For over 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as the upcoming Personal Data Protection Bill. We support the need for heavily regulated industries to stay compliant with these regulations with data erasure solutions that satisfy (and often exceed) those requirements. Contact us today for information on how we can help you prepare for compliance with India's Personal Data Protection Bill.

Learn more about Blancco's Data Erasure Solutions for Enterprise Organizations. Request a free trial today.