

CREATING
RISK
INTELLIGENT
PROFESSIONALS



GRMI

**GLOBAL RISK
MANAGEMENT
INSTITUTE**

Data Privacy | by Govind Kumar (Batch 6)

PROGRAMME
ENDORSED BY



ASSOCIATE
PARTNER



STRATEGIC
PARTNER



ASSOCIATE
MEMBER



STRATEGIC
PARTNER



What is Data Privacy?

Data privacy or information privacy is a branch of data security concerned with the proper handling of data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around:

Whether or how data is shared with third parties.

How data is legally collected or stored.

Regulatory restrictions such as [GDPR](#), [HIPAA](#), [GLBA](#), or [CCPA](#).

Data Privacy Law and Act Timeline

US Privacy Act 1974	US Privacy Act of 1974 maintains restrictions on data held by government agencies
HIPAA 1996	Health Insurance Portability and Accountability Act (HIPAA) protects health information
GLBA 1999	Gramm-Leach-Bliley Act (GLBA) protects financial nonpublic personal information (NPI)
COPPA 2000	Children's Online Privacy Protection Act (COPPA) protects children's data (≤ 12 yrs.)
Privacy Rule 2000	The Privacy Rule fortifies HIPAA and safeguards individuals' private health information
SOX 2002	Sarbanes-Oxley Act (SOX) protects the public from fraudulent practices by corporations
FISMA 2002	Federal Information Security Management Act (FISMA) orders agencies to protect data
ISO 27001 2013	ISO 27001 functions as a framework for an information security management system
GDPR 2018	General Data Privacy Regulation (GDPR) aims to protect EU citizens' personal data
CCPA 2020	California Consumer Privacy Act (CCPA) restricts how companies collect and use data

VARONIS

No Such Law In India

Total Data Records Lost or Stolen by Country



Security incidents related with Personal Data

Written by **Pranav Mukul** , Edited by Explained Desk | New Delhi | Updated: November 12, 2020 9:52:49 am



bigbasket

Cyble has claimed that personal information of as many as 20 million users such as full names, email IDs, password hashes, etc

India's top online grocer BigBasket has suffered a potential data breach **resulting in personal information of over 20 million customers** being allegedly sold on the dark web. This incident follows a series of data breaches that have impacted Indian companies.

Waiting for securepuba

- **Banking:** In January 2019, an SBI server in Mumbai was shown to be unsecured and vulnerable, exposing the data of **millions of its customers**. The server was not password protected, and so information such as account balances, mobile numbers, and even account numbers were effectively on display. SBI secured the server soon afterwards, but this incident emphasised the need for improving digital infrastructure in the banking sector.
- **Aadhaar:** The World Bank and certain digital security firms reported that in 2018 the Aadhar data of citizens was being sold online, with almost **a billion users being affected** in just the first few months of 2018. These leaks were a mixture of overt hacks and unprotected servers or leaky government websites. For example, in 2019 the Jharkhand government's website displayed the Aadhar details of around 100,000 government workers.
- **Whatsapp Pegasus:** In 2019, it was reported the Israeli firm NSOs software *Pegasus* was being used **to spy on 19 individuals**, including journalists and human rights activists. By hacking into their devices via a simple missed call, the attackers gained complete access to the individual's data, including locations, passwords, and even the ability to turn cameras and microphones on.
- **Healthcare:** In 2019, a US cybersecurity firm reported that an unnamed Indian healthcare website was hacked, with the hackers stealing the data of **68 lakh patients and doctors**. The stolen information included patient details, patient case history, doctor information, and other personal information.
- **Credit and debit cards:** In October 2019, a Singapore based cybersecurity firm reported that **13 lakh credit and debit card details** had been stolen, and were now on sale online. It was reported that it was likely that this data stolen by placing a magnetic stripe in an ATM that was able to copy the information of the user's card.

Is there privacy on Internet?

Privacy Policies of Telecom Service Providers

Airtel



- Explicitly states that provision of services is contingent upon consent to process data; may contravene PDPB
- No additional safeguards for sensitive personal data
- Reserves right to process personal data post termination of contract
- Data retention timelines and anonymisation standards not visible
- Unclear whether DND SMS stops messages or stops data collection and sharing
- Does not take consent before sharing data with third parties; may allow them to have lower security standards than itself

Sign language interpretation upon request.

Jio



- Notes that Jio, “may not be able to process your request of correction, updation or deletion, in case... it is extremely difficult to implement”. PDPB may not allow for such exemptions.
- Withdrawal of consent may lead to cancellation of services
- Again, data retention timelines and anonymisation standards not visible
- Also seems to hold its authorised third party partners to lower standards than itself.
- The policy lists ‘hacking’ as a case in which Reliance Jio exempts itself from responsibility in case of a breach of security. Now, the DoT’s user license agreement also specifies that “The LICENSEE shall be completely and totally responsible for security of their networks.”
- Lastly, the ambiguity over whether the DND SMS stops the collection and sharing of data persists here as well.

Sign language interpretation upon request.

Vi



- Seems to view the usage of services as equivalent to the provision of consent for the processing of data. May contravene PDPB as consent may not be free or capable of being withdrawn.
- Does not mention whether the withdrawal for processing certain data is viewed grounds for termination of services by Vi.
- Indicates that Vi may collect data about, "preferences for particular products, services or lifestyle activities".
- Inclusion of user in any telephone or similar directory following an opt-out model
- Sharing of anonymised information with authorised third parties also follows opt-out model
- Yet again, data retention timelines and data anonymisation standards are missing
- Also does not specify any consent sharing any mechanism for sharing data with authorised third parties.
- Ambiguity of the implications of the DND SMS remains here as well
- Vi's policy too seems to imply that it may allow the security standards of the third parties to be lax.

Sign language interpretation upon request.



WHATSAPP PRIVACY POLICY CHANGES



INTERNET
FREEDOM
FOUNDATION

WhatsApp is currently witnessing a mass exodus of privacy concerned users after it released an in-app notification forcing users to accept its revised Privacy Policy by 08 February 2021 or stop using its service entirely.

HOW IT STARTED WHATSAPP IN 2014

"If partnering with Facebook meant that we had to change our values, we wouldn't have done it. Instead, we are forming a partnership that would allow us to continue operating independently and autonomously. Our fundamental values and beliefs will not change. Our principles will not change...Speculation to the contrary isn't just baseless and unfounded, it's irresponsible. It has the effect of scaring people into thinking we're suddenly collecting all kinds of new data. That's just not true, and it's important to us that you know that."

HOW IT'S GOING WHATSAPP TODAY

"The information we share with the other Facebook Companies includes your account registration information (such as your phone number), transaction data, service-related information, information on how you interact with others (including businesses) when using our Services, mobile device information, your IP address, and may include other information identified in the Privacy Policy section entitled 'Information We Collect' or obtained upon notice to you or based on your consent."

info@internetfreedom.com | www.internetfreedom.in

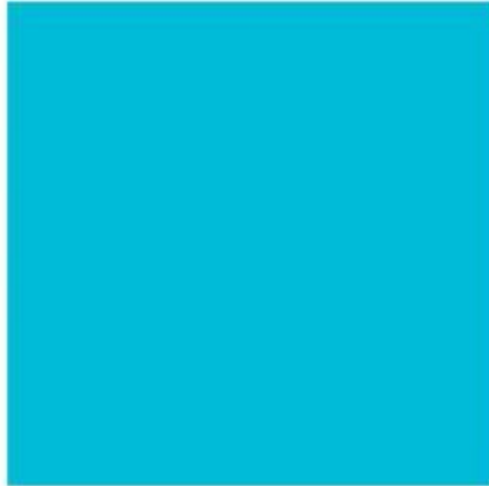
Data Privacy In India

The Indian Privacy Code, 2018 builds off on an incremental process. It takes its foundation and inspiration from the Privacy (Protection) Bill, 2013 which was drafted over a series of roundtables and inputs conducted by the Centre for Internet and Society, Bangalore.

To update and to make it's scope comprehensive it has been drafted by distilling 7 privacy principles from various constitutional and expert texts..

7 Principles

- INDIVIDUAL RIGHTS ARE AT THE CENTER OF PRIVACY AND DATA PROTECTION
- A DATA PROTECTION LAW MUST BE BASED ON PRIVACY PRINCIPLES
- A STRONG PRIVACY COMMISSION MUST BE CREATED TO ENFORCE THE PRIVACY PRINCIPLES
- THE GOVERNMENT SHOULD RESPECT USER PRIVACY
- A COMPLETE PRIVACY CODE COMES WITH SURVEILLANCE REFORM
- THE RIGHT TO INFORMATION NEEDS TO BE STRENGTHENED AND PROTECTED
- INTERNATIONAL PROTECTIONS AND HARMONISATION TO PROTECT THE OPEN INTERNET MUST BE INCORPORATED



Campus Address :

88, Sector 44,
Gurgaon – 122002

CONTACT US

www.grm.institute

Email :
admissions@grm.institute

Thank you!

