As draft Data Protection Bill gets Cabinet nod, here's how other countries protect users' data

With the draft Digital Personal Data Protection Bill, 2022, getting approval from the Union Cabinet and set to be tabled in Parliament, we take a look at how data protection laws protect the data of citizens in other countries.

By Aishwarya Paliwal: The Union Cabinet has approved the draft Data Protection Bill which is expected to be tabled in the upcoming Monsoon session of Parliament for consideration and passage. If passed, the law will become India's core data governance framework, six years after the Supreme Court declared privacy as a fundamental right.

The Digital Personal Data Protection Bill, 2022 is aimed at safeguarding personal data.

Key provisions of the bill include requiring companies collecting data to cease retaining personal information or remove any means by which personal data can be linked to specific data principles.

Consent by individuals is important in most countries before their data can be used. Regulators have focused on the consent of citizens before any exchange of data takes place.

Now, let's take a look at how the data protection laws in some countries are different from the one in India.

ALSO READ | Facebook to Indian Supreme Court: If WhatsApp users want privacy, they should not have Facebook account

UNITED STATES

User consent is primary in the US. One of the defining features of data protection laws in the country is the consent power given to a citizen.

The US has a Privacy Act in place since 1974, which governs how federal agencies can collect and use data about individuals in its system of records.

For instance, if you are a US citizen, the government cannot disclose personal information without written consent from the individual, subject to limited exceptions.

Individuals reserve the right to request or change their records if they are inaccurate or incomplete and to be protected against unwarranted invasion of their privacy.

The US also has a law protecting the health data of patients. The Health Insurance Portability and Accountability Act (HIPAA) was signed into law by then President Bill Clinton in 1996.

HIPAA mandates how healthcare providers can use a patient's personal health data. The regulations only apply to covered entities, which encompasses providers (like doctors, nurses, psychologists and dentists), health plan (including healthcare insurance companies and government plans like Medicare) and healthcare clearinghouses, which process medical information.

The guidelines prescribe that covered entities must comply with an individual's right to see their health information and correct their health information. The covered entities cannot use or share health information without the individual's written consent.

So, this means, as a US citizen, if your healthcare provider (doctors, nurses, psychologists and dentists) is misusing your data, you can sue the provider under the HIPAA.

EUROPE

Europe is governed by GDPR (General Data Protection Regulation) Act. This EU law mandates rules for how organisations and companies must use the personal data of citizens.

If you are a citizen living in the EU, you should report any personal data breach within 72 hours.

Companies in Europe should assign a Data Protection Officer (DPO) in their organisations. The DPO should work as the main operator and the expert in organisations' privacy work. The officer should report to the data protection authority in the country where the organisation is established.

If a citizen feels that his/her personal information such as health or financial data, is breached, the incident must be reported to the authorities within 72 hours.

ASIA

In countries like China, Japan and Hong Kong, data protection laws vary slightly. Some nations have boards like the one India is planning to set up. These boards settle grievances.

Citizens of these countries are asked by companies about their consent. The companies have to specify the usage of data and also have to delete the data once its usage is over. One can sue the companies if any breach happens.

WHAT'S DATA PROTECTION BOARD?

To oversee the implementation of the law in India, a Data Protection Board will be established by the government. This board will function as an adjudicatory body to address privacy-related grievances and disputes between parties.

The Centre will appoint the chief executive of the board and board members. The bill is expected to allow "voluntary undertakings", where platforms that have violated the law can bring their case before the data protection board. The board will have the authority to accept settlement fees and determine the penalty amount.

The maximum penalty for a data breach by a platform has been set at Rs 250 crore per instance. However, the interpretation of "per instance" remains subjective and could refer to either a single data breach or the number of individuals affected by it multiplied by Rs 250 crore.

Citizens will now be able to go to the board with a grievance and get it settled. The penalty will be decided on a case-to-case basis.