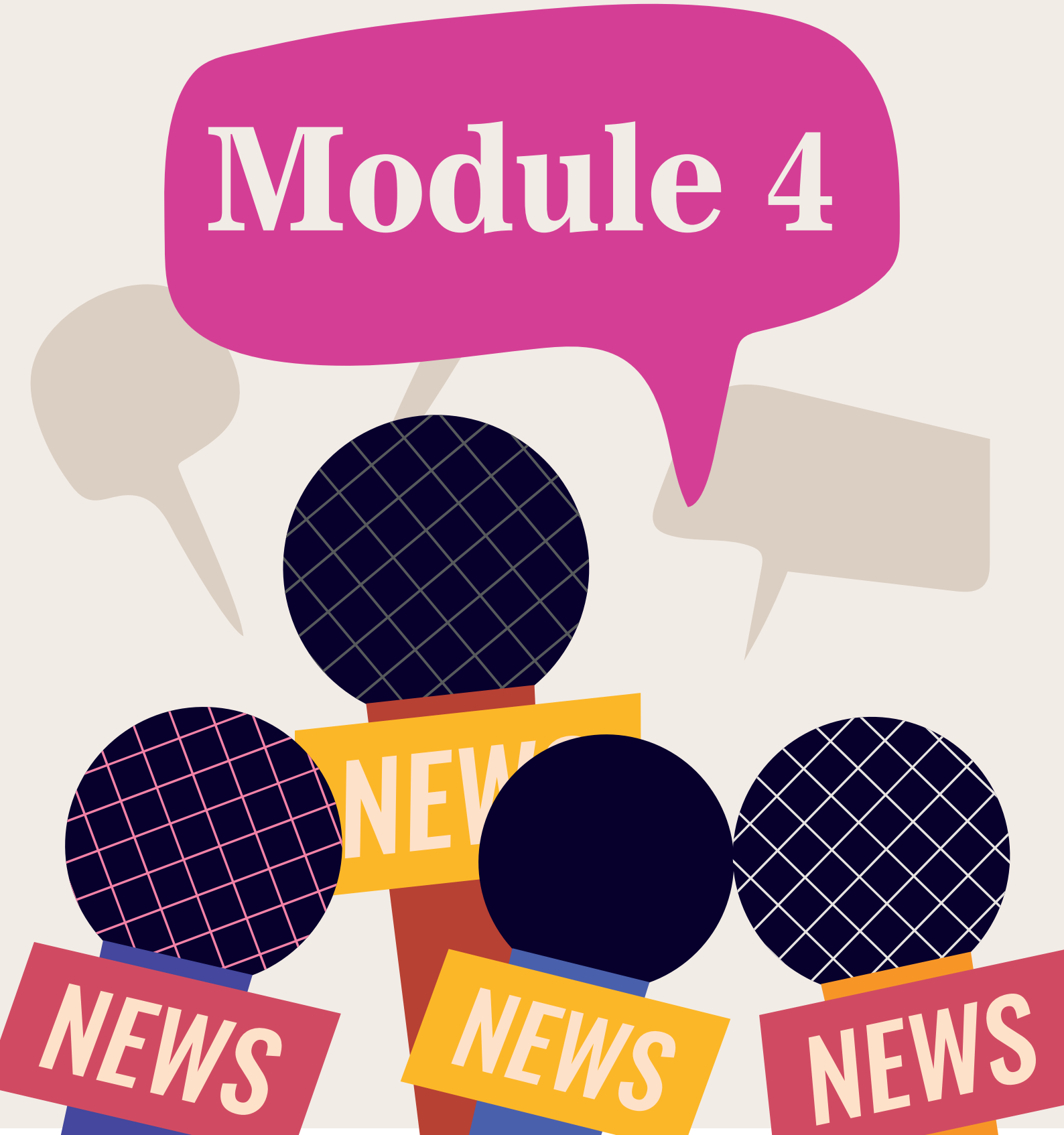
Talking Data to the Fourth Pillar

DIGITAL EMPOWERMENT foundation

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Talking Data to the Fourth Pillar

Module 4



Talking Data to the Fourth Pillar

April 2023

Author: Dushyant Arora

Concept: Vineetha Venugopal

Review: Vineetha Venugopal, Jenny Sulfath, and Arpita Kanjilal

Advisor: Osama Manzar

Design and Illustration: Yuvasree Mohan

Published and distributed by:

Digital Empowerment Foundation
House No. 44, 2nd and 3rd Floor (next to Narayana IIT Academy)
Kalu Sarai (near IIT Flyover)
New Delhi – 110016 Tel: 91-11-42233100 / Fax: 91-11-26532787
Email: def@defindia.net | URL: www.defindia.org

INTRODUCTION

The last few years have seen increasing digital surveillance on citizens by various national governments and corporates as evidenced by Cambridge Analytica and the Pegasus project. With existing legal provisions inadequate to ensure the privacy and autonomy of the citizenry in a digitalized world, many countries are legislating on digital data protection. However, with the rise of authoritarian politics and the digital economy, there is also the danger of these legislations prioritizing state surveillance and commodification of data over the rights of the people.

Particularly vulnerable are the journalists. Termed the fourth estate by the British parliamentarian Edmund Burke, the media would later be termed the fourth pillar of democracy meant to scrutinize the executive, judiciary, and legislature on behalf of the people. Due to the particularity of their profession, journalists need to protect not only their privacy, but also that of their sources, making them even more vulnerable. As such, it is important that journalists are equipped with the knowledge to safeguard themselves using digital and legal means.

India is currently on the 4th iteration of its data protection legislation having closed the public consultation for the draft Digital Data Protection Bill, 2022 as of January 2023. However, the draft bill has been critiqued for facilitating state surveillance without adequate safeguards. There are also fears that vague terms in the bill can be interpreted in a manner that would be detrimental to the freedom of expression, freedom of the press and privacy.

It was in this context that Digital Empowerment Foundation initiated the program 'Talking Data to the Fourth Pillar'. This cohort-based learning program was designed with the aim of discussing core concepts on privacy, data protection and online safety so that the trained participants can

- Educate and inform the citizenry through content/art pieces
- Use the legal knowledge acquired from training to safeguard journalistic freedoms
- Practice responsible reporting that is respectful of citizen's privacy and data
- Exchange best journalistic practices and collectively work towards securing online Privacy and safety

Additionally, women, queer individuals and other marginalized communities have been historically oppressed by surveillance and data processing. All these calls for nuanced understandings of privacy and data protection from an intersectional feminist perspective. It is our hope that the sessions and discussions will contribute to fostering such an understanding. We look forward to learning with you and learning from you.

- Vineetha Venugopal

While a right to privacy has been recognised by the Indian Supreme Court in 2017, most of India's current data privacy protection laws exist primarily in the Information Technology Act, 2000 ('the IT Act'). Surveillance is also governed in part by the antiquated and obviously outdated 1885 Telegraph Act.

Data privacy protection stipulations are also contained in rules imposed by various regulatory authorities. These include rules imposed by the RBI, the Telecom Regulatory Authority of India (TRAI), the Insurance Regulatory and Development Authority of India, Securities and Exchange Board of India (SEBI), Pension Fund Regulatory and Development Authority and Unified Licence Agreements issued pursuant to the National Telecom Policy, 2012 by the Department of Telecommunications (DOT).

Information Technology Act, 2000 ('the IT Act')

The Indian IT Act, 2000 is the primary source of law around e-commerce, digital transactions and cybercrime. It provides legal sanction to digital commerce and transactions, allows e-governance and helps prevent and penalise cybercrimes. It also deals with the authentication of e-signatures and electronic documents.

The Indian Information Technology (IT) Act, 2000 includes several provisions related to data protection, including:

Section 43A - This section deals with compensation for failure to protect sensitive personal data.

Section 72A - This section deals with punishment for disclosure of information in breach of lawful contract.

Section 69 - This section empowers the government to issue directions for

interception or monitoring or decryption of any information through any computer resource.

This section reads: "Power to issue directions for interception or monitoring or decryption of any information through any computer resource. -

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource."

This section also stipulates a punishment of 7 years imprisonment and the payment of a fine in the case of non-cooperation with authorities in handing over requested data.

Section 72 - This section deals with punishment for breach of confidentiality and privacy, stipulating a two-year jail sentence, and/or a fine of up to 1 lakh rupees.

Section 66E - This gender-neutral section deals with punishment for violation of privacy of an individual, particularly the "capturing, publishing or transmitting of the image of a private area of any person without his or her consent". This would carry a punishment of a jail term of up to three years, and/or a fine of up to two lakh rupees.

Section 65B - This section lays down the procedure for authentication of electronic records.

Section 79 - This section provides immunity to intermediaries for third-party information, subject to conditions.

The Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021)

In October 2021, the government of India notified amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, **2021 (IT Rules, 2021).** These rules were widely criticised as they intended to classify digital news platforms as "publishers of news and current affairs content". The rules thereby sought to regulate such platforms as news platforms, requiring them to conform to a Code of Ethics and government oversight, which mandated that the content be "in good taste", "decent" and other vague normative terms that could be misinterpreted or misused to censor digital news platforms arbitrarily.

Under ***Rule 11 of the IT Rules, 2021,*** every non-newspaper news website and/or blog/youtube channel/newsletter/podcast is to appoint a 'grievance officer' who will have to 'acknowledge' every grievance anyone has about anything published, posted or hosted on their platform in less than 24 hours, and then 'resolve' it within 15 days. Imagine this- lakhs of workers of a political party/corporate/film actor/spiritual baba get upset about a news item critical of the subject of their worship. They send lakhs of grievances. How will a person running a newsletter about law/media/science or even a news website or a weekly podcast respond to all of this?

Rule 12 demands that groups of publishers to establish a self regulation body which will be headed by a retired High Court or Supreme Court Judge "or an independent eminent person from the field of media, broadcasting, entertainment, child rights, human rights or such other relevant field and have other members, not exceeding six, being experts from the field of media, broadcasting, entertainment, child rights, human rights and such other relevant fields." This self-regulation body must register itself with the government. The government will have the final say on the composition of these bodies: if it doesn't like someone, that person won't be able to become a member. Commentators have warned that such a body would be staffed only by people who are sympathetic to the political party in power.


IT
Rules
2021

The government will then "publish a charter for self regulating bodies, including Codes of Practices for such bodies"; "issue appropriate guidance and advisories to publishers;" "issue orders and directions to the publishers for maintenance and adherence to the Code of Ethics."

This self regulatory body is supposed to be the body to which appeals from the original grievance officer will go.

Finally, the IT Rules call for the formation of the top-most body, or the "Inter-Departmental Committee" Rule 14 states that "The Ministry shall constitute an Inter- Departmental Committee, called the Committee, consisting of representatives from the Ministry of Information and Broadcasting, Ministry of Women and Child Development, Ministry of Law and Justice, Ministry of Home Affairs, Ministry of Electronics and Information Technology, Ministry of External Affairs, Ministry of Defence, and such other Ministries and Organisations, including domain experts, that it may decide to include in the Committee"

A body of bureaucrats from multiple ministries will spend their time resolving 'grievances' people have with news websites, youtube videos, podcasts, etc. This body has been given the power to ask any publisher to delete any content it doesn't like, without hearing from the publisher of the content.

Rule 16 of the IT Rules, 2021 also deals with the government's right to block content in the country. Rule 16 states, "In case of emergency nature, the Secretary, Ministry of Information and Broadcasting may, if he is satisfied that it is necessary or expedient and justifiable for blocking for public access of any information or part thereof through any computer resource and […] as an interim measure issue such directions as he may consider necessary to such identified or identifiable persons, publishers or intermediary in control of such computer resource hosting such information or part thereof without giving him an opportunity of hearing." This was the rule invoked by the government when it recently blocked access to a BBC documentary engaging with PM Modi's alleged complicity in the 2002 Godhra riots, India: The Modi Question.

Rule 4(2) of the rules reads: "….A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under section 69 by the Competent Authority as per the Information Technology (Procedure and Safeguards for interception, mon-

itoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form…."

The fundamental principle behind 'encrypting' messages is to protect the contents of the message and the identity of the sender. Such encryption is also consistent with the landmark judgement of the Supreme Court of India in Justice K. S. Puttaswamy v. Union of India which held that Privacy is a fundamental right.

To comply with Rule 4(2) would mean that companies like Whatsapp would have to destroy the business model or create a new product only for India. If this happens India would be the only democracy if not the only country across the world to have such a policy.

This will also significantly and adversely affect independent journalism since many journalists use encrypted messaging services to share documents and other information. Democracy will be throttled. Similarly, it will also be detrimental to peaceful protests by civil society.

While the 'provisos' or explanations to the aforementioned rule do say:

"..Provided that an order shall only be passed for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material, punishable with imprisonment for a term of not less than five years:

Provided further that no order shall be passed in cases where other less intrusive means are effective in identifying the originator of the information

Provided also that in complying with an order for identification of the first originator, no significant social media intermediary shall be required to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users.. "

But phrases like "public order" are vague. They are not just 'susceptible' or 'prone' to abuse but there is sufficient reportage and research that says there is an epidemic of abuse by state of such vague phraseology to routinely persecute innocent critics and political opponents.

Under the Criminal Procedure Code, police authorities have powers to seize phones. However, the most significant difference between these powers and the power under the IT rules is that when the police seizes someone's phone, the person in question knows that his phone is with the police. There are several sections in the Code which obligate the police to get a warrant before searching/seizing someone's phone.

Therefore, at least in theory, and many times in practice, the police's powers a) can not be exercised without the owner of the information/device finding out b) In some cases require prior permission from court c) Because there is information, the person whose phone is being accessed by the police can go to court and challenge the legality of the search/seizure.

In the case of the IT rules there is no provision whatsoever of information/notice to the person whose information is being taken. Neither prior to such information being obtained nor after it is obtained.

Digital Personal Data Protection Bill, 2022

Given how quickly the world's digital ecosystem has grown and changed, the Indian IT Act 2000 has been found woefully inadequate to deal with new digital challenges and threats to data privacy. It was found particularly ill-equipped to address data collection, storage, (mis)use and surveillance by tech giants such as Meta and Twitter. In order to address these gaps and create a more comprehensive, robust legal framework to address personal data protection, India is currently in the process of finalising a draft of its own controversial new Digital Personal Data Protection Bill. In November 2022, the government of India released a second draft of the Bill, shortly after withdrawing a previous draft version of the Bill released in August 2022. The draft bill is still being discussed with various stakeholders before being voted on in Parliament.

The draft bill states that the proposed law applies only to personal data that is collected either online, or offline where the personal data is in a digitised format.

Regarding personal data, the Bill states that consent to share that personal data must 'freely given', "specific', 'informed' and an 'unambiguous indication of consent' through a 'clear affirmative action' by the data subject. Data subjects, or the person from whom data is being collected, has the right to know what data is being processed, and has the right to correct their own personal data. They can also have their personal data erased if the data no longer serves the purpose for which it was collected.

The Bill mandates that data subjects be presented with an itemised disclosure of the types of personal data being collected, and the purposes for which that data is being collected.

The draft law refers to entities known as Significant Data Fiduciary (SDF). Data fiduciaries are entities that determine the purpose of any personal data and the means of processing it. Under this draft bill, some entities are to be designated SDF by the Government. The government determines whether an entity should be granted SDF status based on criteria relating to the volume of data collected, the risk of harm, and, interestingly, the potential impact on the sovereignty and integrity of India and the risk to electoral democracy.

Data fiduciaries must appoint a contact person to whom a data subject can contact for data privacy-related complaints or issues, publish a grievance redressal procedure, and address complaints around data privacy within 7 days of receipt of complaint. SDFs must appoint a data protection officer, and an independent data auditor to audit data protection compliance in accordance with the law.

Data fiduciaries under this draft Bill must obtain parental consent before processing personal data of children below the age of 18. Under the provisions of this Bill, data fiduciaries must also not track or engage in behavioural monitoring of children, nor target ads to them. The global standard, however, around the age of adulthood when entering digital spaces, is often taken to be 16 years.

Criticisms of the Digital Personal Data Protection Bill, 2022

The Digital Personal Data Protection Bill, 2022 has come under criticism for a variety of reasons. It provides sweeping exemptions for the government from the mandates of the Bill's data protection framework for vague, broad reasons that have not been clearly defined in the Bill. These reasons include the protection of "interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, [or] maintenance of public order." These exemptions could easily be misused by the government in power to surveil and harass citizens.

The draft Bill has also been criticised for failing to allow for an independent body to oversee and monitor the sweeping exemptions and powers it grants the government. It instead allows for a Data Protection Board, composed of individuals selected or removed from service by the government. Human Rights Watch has warned that this "absence of checks would facilitate surveillance and possible mass violations of people's privacy."

The law provides an exemption for the processing of data in India of individuals located outside India under a cross-border contractual arrangement. This is expected to cover individuals involved in the offshore outsourcing industry.

The law also stipulates that data should not be stored once the purpose for which the data was collected is no longer relevant being served, and if the data is no longer required for legal or business reasons. However, the government of India is exempt from these obligations, and can retain the data it has collected long after the purpose of that data collection has been served.

While the proposed draft Bill contains stipulations regarding fines for noncompliance with its diktats, these fines are not linked to the turnover of the entity in question, and are capped at up to 50 million rupees (around 60 million dollars), depending on the violation.

The GDPR - The "gold standard" of data privacy protection

The General Data Protection Regulation (GDPR) is a comprehensive data privacy regulation that applies to organisations operating in the European Union (EU). It claims to be "the toughest privacy and security law in the world." The regulation came into effect on May 25, 2018, and replaces the 1995 EU Data Protection Directive.

The General Data Protection Regulation (GDPR) is considered the gold standard of data privacy protection because it provides a comprehensive framework for the protection of personal data, grants individuals strong rights related to their personal data, and imposes strict enforcement measures to ensure compliance. It is considered particularly robust because it allows for:

Comprehensive coverage: The GDPR applies to all organisations operating in the European Union (EU), regardless of size or location, and provides a comprehensive framework for the protection of personal data.

Strong consumer rights: The GDPR grants individuals several rights related to their personal data, including the right to access, the right to erasure, and the right to data portability.

Strict enforcement: The GDPR imposes significant fines for non-compliance, including fines of up to 4% of a company's global revenue or 20 million euros, whichever is higher. This provides a strong incentive for organisations to comply with the regulation.

Focus on privacy by design: The GDPR requires organisations to implement appropriate technical and organisational measures to protect personal data, and to design their systems and processes with privacy in mind, as opposed to piecemeal or case-by-case privacy protections.

Harmonisation of privacy laws: The GDPR harmonises data privacy laws across the EU, creating a single set of rules for organisations operating in the

region. This reduces complexity and makes it easier for organisations to comply with the regulation.

The GDPR lays out specific rules around the collection, processing, and storage of personal data, including:

Consent: The GDPR requires organisations to obtain clear and specific consent from individuals before collecting their personal data.

Transparency: Organisations must provide clear and concise information about how personal data will be used, including the purpose of processing, the length of time it will be stored, and who will have access to it.

Right to Access: Individuals have the right to access their personal data and to receive a copy of it.

Right to Erasure: Individuals have the right to request the deletion of their personal data in certain circumstances.

Data Breach Notification: Organisations must notify the relevant authorities within 72 hours of becoming aware of a data breach.

Fines: The GDPR imposes significant fines for non-compliance, including fines of up to 4% of a company's global revenue or 20 million euros, whichever is higher.

References:

https://www.dataguidance.com/notes/india-data-protection-overview
https://www.huntonprivacyblog.com/2022/11/22/india-releases-fourth-draft-of-data-protection-bill/
https://www.mondaq.com/india/privacy-protection/1258868/whats-in-indias-new-data-protection-bill
https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill/
https://www.indiatoday.in/india/story/why-government-withdrew-bill-it-brought-to-protect-your-data-1983734-2022-08-04
https://indianexpress.com/article/explained/explained-economics/india-draft-digital-privacy-law-data-protection-laws-8279199/
https://www.livemint.com/news/india/explainer-data-protection-bill-significance-criticism-all-you-neeed-to-know-11659530273031.html
https://www.atlanticcouncil.org/blogs/southasiasource/indias-new-data-bill-is-a-mixed-bag-for-privacy/
https://www.orfonline.org/research/the-draft-digital-personal-data-protection-bill-2022/#:~:text=Section%2017%20of%20the%20draft,be%20specified.%E2%80%9D%20This%20is%20a
https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance#:~:text=The%20Digital%20Personal%20Data%20Protection,was%20dropped%20in%20August%202022.
https://gdpr.eu/what-is-gdpr/
https://www.itlaw.in/
https://thewire.in/media/why-the-wire-wants-the-new-it-rules-struck-down
https://www.theguardian.com/world/2023/jan/23/india-emergency-laws-to-ban-bbc-narendra-modi-documentary
https://www.thehindu.com/sci-tech/technology/explained-the-amendments-to-the-it-rules-2021/article66079214.ece
https://prsindia.org/theprsblog/explained-draft-amendments-to-the-it-rules-2p;021

Notes

Notes

Notes

Talking data to the fourth pillar

defindia.org

No# 44, 2nd & 3rd Floor, Kalu Sarai,
Near Naraina IIT Academy, Delhi 110017
info@defindia.org

Talking data to the fourth pillar