Government of West Bengal
Department of Information Technology & Electronics
Moni Bhandar, 5th and 6th Floor, Sector V, Block EP&GP,
Salt Lake, Kolkata 700091.
Phone: 2357-2545, Fax: 2357-2534.

NOTIFICATION

No- 1281-Estt/ITE-20013/2/2023 Dated: 17.11.2023.

WHEREAS, data can be defined as any discrete and objective piece of information which encompasses a wide array of forms such as text, numbers, images, audio, video etc that collectively fuel our digital interactions in day to day life;

AND WHEREAS, data can be categorised in to two main types viz. structured data which is highly organised and easily processed while unstructured data which is complex and requires advanced techniques for analysis;

AND WHEREAS, data privacy refers to the protection of individuals' personal information and the control they have over its collection, storage and dissemination which is the fundamental concept that ensures right to keep sensitive data out of the wrong hands;

AND WHEREAS, it is felt to empower individuals, government sectors and organizations to protect sensitive information and build trust in our increasingly data centric world;

NOW THEREFORE, the Governor is pleased to notify the 'West Bengal Data Privacy Guidelines, 2023' (attached herewith) which will empower individuals, government bodies and organisations to take charge of their own data, the data in rest and controlled by them in a responsible and ethical manner. Whereby the guidelines shall be implemented through WBEIDC Ltd. (Webel), being the State Implementing Agency (SIA) and State Level Nodal Agency(SLNA).

This has the approval of the competent authority of this Department vide Diary No. 214 dated 17.11.2023.

Enclosure: As stated.

By order of the Governor,

Principal Secretary to the
Government of West Bengal

O/C

No. 1281/1(85)–Estt/ITE-20013/2/2023 Dated: 17.11.2023

Copy forwarded for kind information and necessary action to:-

- The Secretary to the Government of India, Department of Telecommunications, Sanchar Bhawan, New Delhi.
- The Secretary to the Government of India, Ministry of Electronics & Information Technology, 6, CGO Complex, New Delhi-110003.
- The Additional Chief Secretary/ Principal Secretary/ Secretary,_____Department(all), Government of West Bengal.
- The Managing Director, WBEIDC Ltd., Webel Bhavan, Block: EP & GP, Sector-V, Salt Lake City, Kolkata- 700091.
- The Managing Director, WBIDC, 23, Abanindranath Tagore Sarani, 'Protiti', Kolkata- 700017.
- The Managing Director, WBIIDC, Block- DJ, Plot No. 10, Sector-II, Salt Lake City, Kolkata-700091.
- The Managing Director, WBSIDCL, 31, Black Burn Lane, 4th Floor, Shilpa Bhavan, Kolkata-700012.
- The Managing Director, WBHIDCO, Premises No. 35-1111, Biswa Bangla Sarani, 3rd Rotary, New Town, Kolkata- 700156.
- The Chief Executive Officer, Webel Technology Limited, BP-5, Sector-V, Salt Lake City, Kolkata- 700091.
- The District Magistrate,_____, District (all), West Bengal.
- The OSD to the Chief Secretary, Government of West Bengal.
- The PS to the Hon'ble MIC, IT&E Department, Government of West Bengal.
- The SPA to the Principal Secretary, IT&E Department, Government of West Bengal.

17/11/2023

Additional Secretary to the Government of West Bengal

No. 1281/1(85)/2(13)–Estt/ITE-20013/3/2023 Dated: 17.11.2023

Copy forwarded for information only to:

- The Director General, Digital Infrastructure Providers Association (DIPA), 2nd& 3rd Floor, 7, Bhai Veer Singh Marg, Gole Market, New Delhi- 110001.
- The Director General, COAI, Sector- 2, Bhai Veer Singh Marg, Gole Market, New Delhi- 110001.
- The Director, STPI, Kolkata, Webel STP 2 Building, 2nd Floor, DN-53, Sector-V, Salt lake, Kolkata- 700091.
- The Regional Director (East), NASSCOM RO East, Infinity Business Centre, Infinity Benchmark, Room No. 605, 6th Floor, Block-EP&GP, Plot- G1, Sector-V, Salt lake, Kolkata- 700091.
- The President, BCC&I, 6, Netaji Subhas Road, Kolkata- 700001.
- The President, COMPASS, 37, Shakespear Sarani, Kolkata- 700017.
- The President, TIE, Infinity Benchmark, Infinity Business Centre, 6th Floor, Suite# 607, Plot-GP, Sector-V, Salt lake, Kolkata- 700091.
- The Associate Vice President, Internet & Mobile Association of India, 232-B, Ground Floor, Okhla Industrial Estate, Phase-III, New Delhi- 110020.
- The Director, FICCI, Dhanseri House, 4A, Woodburn Park, Kolkata- 700020.
- The Director, CII, 6, Netaji Subhas Road, Kolkata- 700001.
- The Director General & CEO, AMCHAM, PHD House, 4th Floor, 4/2, Siri Institutional Area, August Kranti Marg, New Delhi- 110016.
- The Director (East &North East), ASSOCHAM, 18, Ballygunge Circular Road, Kolkata- 700019.
- The Chairman, Electronics and Computer Software Export Promotion Council, Ground Floor, Building No. DN-53, STP-II Building, Salt lake, Kolkata- 700091.

17/11/2023

Additional Secretary to the
Government of West Bengal

WEST BENGAL DATA PRIVACY GUIDELINES, 2023

Department of Information Technology & Electronics,
Government of West Bengal

Notified vide No. 1281-Estt/ITE-20013/2/2023 Dated 17.11.2023

TABLE OF CONTENTS

PREFACE 2
PRINCIPLES OF DATA PRIVACY 3
STAKEHOLDERS IN WORLD OF DATA PRIVACY 4
DIGITAL PERSONAL DATA EXPLAINED 5
ABOUT CONSENT 6
What is consent? 6
Why is consent important? 6
How to give consent? 6
INFORMED DECISION MAKING 7
DOS & DON'TS OF DATA FIDUCIARIES 8
DOS & DON'TS OF DATA PRINCIPAL 9
DATA RETENTION 10
How to follow data retention to abide by data privacy guidelines? 10
DATA ANONYMIZATION 11
What is data anonymization? 11
How to ensure data anonymization and adhere to data privacy? 11
EXEMPTIONS 12
RESOURCE CREATION AND CAPACITY BUILDING 13
IMPLEMENTATION FRAMEWORK 14

PREFACE

"Data is the new oil" - Clive Humby

In an era where information flows seamlessly through the digital arteries of our interconnected world, data has become a cornerstone of modern life. It permeates every facet of our existence, from personal communication to business operations, scientific advancements to political decision-making and policy making. Data is the lifeblood of the digital age, and its significance cannot be overstated.

Data can be defined as any discrete and objective pieces of information. It encompasses a wide array of forms, such as text, numbers, images, audio, and video, which collectively fuel our digital interactions. Data can be categorized into two main types: structured data, which is highly organized and easily processed, and unstructured data, which is more complex and requires advanced techniques for analysis.

As our reliance on data continues to grow, so does the paramount concern for data privacy. Data privacy refers to the protection of individuals' personal information and the control they have over its collection, storage, and dissemination. It is the fundamental concept that ensures our right to keep sensitive data out of the wrong hands. This includes not only personal details like names and addresses but also the patterns of our online behavior, our financial information, and even our health records.

In today's digital landscape, the need for data privacy has been more critical than ever before. With the proliferation of data-driven technologies, there is a constant exchange of data between individuals, businesses, and governments. This exchange, however, brings with it the potential for misuse and abuse of personal information. The consequences of data breaches and privacy violations can be dire, ranging from identity theft to erosion of trust in institutions.

Hence, the importance of this document lies in its exploration of data privacy – to empower individuals, government bodies and organizations to protect sensitive information and build trust in our increasingly data-centric world. Understanding the nuances of data privacy, its regulations, and best practices is a crucial step in navigating the complex landscape of our digital age. By shedding light on these aspects, we aim to contribute to the ongoing discourse on safeguarding our digital identities, fostering responsible data handling, and advocating for the rights of data subjects.

This document, therefore, serves as a valuable resource to demystify the world of data privacy and empower individuals, government bodies and organizations to take charge of their data in a responsible and ethical manner. Through knowledge and informed action, we can collectively ensure that data remains a force for good, benefitting society while respecting the fundamental right to privacy.

PRINCIPLES OF DATA PRIVACY

PRINCIPLE 01

The principle of consented, lawful and transparent use of personal data

PRINCIPLE 02

The principle of purpose limitation (use of personal data only for the purpose specified at the time of obtaining consent of the Data Principal).

PRINCIPLE 03

The principle of data minimization (collection of only as much personal data as is necessary to serve the specified purpose).

PRINCIPLE 04

The principle of data accuracy (ensuring data is correct and updated).

PRINCIPLE 05

The principle of storage limitation (storing data only till it is needed for the specified purpose).

PRINCIPLE 06

The principle of reasonable security safeguards.

PRINCIPLE 07

The principle of accountability through adjudication of data breaches.

STAKEHOLDERS IN WORLD OF DATA PRIVACY

DATA PRINCIPALS

Individuals or organizations whose personal data is being processed.

In essence: Owner of the data

Who can be Data Principals?

- ✓ Individual citizens
- ✓ Organizations
- ✓ Government & Government bodies

DATA FIDUCIARY

Anyone deciding what data will be collected, how it will be collected and the purpose of its use.

Who can be Data Fiduciary?

- ✓ Organizations
- ✓ Government & Government bodies

CONSENT

Give explicit permission for manage , review and use personal data

Who can give consent?
Individual citizens, organizations, Government & Government bodies whose data will be used by data fiduciary.

CONSENT MANAGER

Anyone who assists Data Principals and Data Fiduciaries to give, manage, review and withdraw consent

Who can be Consent Manager?

Person registered with Data Protection Board

DATA PROCESSOR

Anyone who processes data on behalf of Data Fiduciaries based on their instructions.

Who can be Data Processor?

- ✓ Organizations
- ✓ Government & Government bodies

DIGITAL PERSONAL DATA EXPLAINED

Digital personal data encompasses a wide range of information in a digital format that can identify an individual. This includes basic identifiers, online profiles, financial and health information, employment details, online behavior, geolocation data, communication records, and more.

- Basic Identifiers: A person's name, date of birth, physical address, email address, and phone number
- Online Identifiers: Usernames, social media profiles, IP addresses, Mac addresses and device IDs
- Biographical Information: Gender, nationality, and marital status
- Financial Details: Bank account numbers, credit and debit card information, and financial transaction records
- Health and Medical Information: Medical records, health insurance details, and health-related app data
- Employment Information: Job titles, workplace, and salary details
- Digital Behavior and Preferences like Data related to an individual's online activities, search history, purchase history, and preferences in websites, apps, or products
- Social and Relationships: Data about an individual's family, friends, and social connections
- Geolocation Data: Information that can reveal an individual's location through GPS or other tracking technologies
- Communication Data: Emails, messages, and call logs

ABOUT CONSENT

What is consent?

Consent means a person's voluntary agreement to let an organization or individual or government collect and use their personal data for specific purposes. This agreement must be freely given, informed, specific, reversible, and documented, and it has special rules for children's data.

Consent should be specific to each data processing activity. It should not be bundled together with unrelated purposes, and individuals should have a clear understanding of what they are consenting to. Ambiguous or overly broad consent is not considered valid. Also, in case of collecting data of children or differently abled persons, some additional rules like taking consent of their local guardian will apply.

Why is consent important?

- ✓ Empowers individual control by allowing people or organization or government to decide how their personal data is used
- ✓ Ensures compliance required by data privacy laws and regulations
- ✓ Promotes transparency by encouraging clear and open communication between data controllers and data principals and minimizes unnecessary data collection
- ✓ Upholds ethical data handling by encouraging fair and respectful treatment of personal data

How to give consent?

- ✓ The consent should be established through a clear affirmative action by the Data Principal
- ✓ When processing a minor's personal data, consent from their legal guardian needs to be taken
- ✓ Data Principals have the authority to withdraw their consent at any point during the processing
- ✓ Provisions should be there to take consent in local languages also, means the terms and conditions should also be written in local languages as well

INFORMED DECISION MAKING

It is important for the Data Principals to make an informed decision pertaining to sharing their data, the purpose of the data use, duration and so on. A privacy notice is a document that informs the data principals about how their personal data will be collected and used by an organization or government or any entity. Its importance lies in promoting transparency, enabling informed consent, complying with legal requirements, empowering data principals to exercise their data rights, demonstrating accountability, and mitigating legal and financial risks for the organization or government or individual (both data principal & data fiduciary).

Q. Who is responsible to furnish privacy notice while data collection?

A. Data Fiduciary

Q. Who will provide response to privacy notice?

A. Data Principal

Q. Should the privacy notice have details of filling a complaint in case it is required?

A. Yes

DOS & DON'TS OF DATA FIDUCIARIES

- ✓ Implement technical and organizational security safeguard measures to safeguard personal data
- ✓ Determine legal ground of processing and obtain consent from Data Principals where required
- ✓ Provide a privacy notice while obtaining consent from Data Principals
- ✓ Implement a mechanism for Data Principals to exercise their rights
- ✓ Implement a grievance redressal mechanism for handling queries from Data Principals and have an officer (Data Protection Officer) to respond to queries from Data Principals
- ✓ Sign a valid contract with Data Processors to ensure key obligations are abided by them, including timely deletion of data
- ✓ Data Fiduciaries have a responsibility to irrecoverably delete personal data once the purpose for its collection is achieved
- ✓ Data Fiduciaries have a responsibility to irrecoverably delete personal data when the Data Principal withdraws their consent
- ✓ Data Fiduciary is required to inform the Data Protection Board and the Data Principals regarding data breaches

In addition to above, **a Significant Data Fiduciary** (Organization or Government that processes large volume of sensitive data) must also

- ✓ Appoint a Data Protection Officer based in India
- ✓ Appoint an independent data auditor and conduct periodic data audits
- ✓ Conduct Data Protection Impact Assessment periodically

DOS & DON'TS OF DATA PRINCIPAL

- ✓ Data Principals are entitled to access information related to the processing of their data, encompassing the categories of personal data shared and the identities of all Data Processors with whom their personal data has been shared

- ✓ Data Principals possess the authority to halt data processing by revoking their consent through Consent Manager

- ✓ Data Principals can request Data Fiduciaries to rectify, supplement, update, or delete their personal data

- ✓ Data Principals retain the right to seek redressal for their grievances. Data Fiduciaries and Consent Managers must designate qualified individuals (Data Protection Officer, if required) to handle these grievances

- ✓ In the event of incapacity or the demise of the Data Principal, they may designate or nominate a representative to exercise their rights on their behalf

In case of processing personal data of children and differently abled persons it is mandatory to obtain consent from their legal guardians

DATA RETENTION

Data retention is the practice of preserving data for a specific period to meet technical, business, or regulatory requirements. The data should be retained as per data retention schedule which is varied depending upon:

- Criticality level of case
- The purpose of data use and retention
- The nature or type of data in consideration – business or personal or public data
- Legality of the department or organization collecting, processing, and retaining data

How to follow data retention to abide by data privacy guidelines?

- ✓ Data Fiduciary shall itself or direct the Data Processor, to erase personal data as soon as the Data Principal withdraws consent or the purpose of data use is achieved whichever is earlier, unless retention is necessary for compliance with any law

Based on international standard practices, data retention period for different types of data will be as follows:

CATEGORY	RETENTION PERIOD (Data Centre & DR site)	TOTAL RETENTION PERIOD (Including archival)
Medical Records	3 years	25 years (inclusive of the 3 years) Or based on applicable regulations
HR Records	3 years	25 years (inclusive of the 3 years) Or based on applicable regulations
Medical & Security Assistance Case Records	2 years	3 years (inclusive of the 2 years)
Call Recordings	1 year	2 years
Audit logs	3 months	2 years
Corporate Secretariate Record	Life of the entity	Life of the entity + 50 years
Accounting & Financial Records	2 years	7 years or based on applicable regulations
Procurement & Contract Record	Contract Duration	Contract duration + 7 years or based on applicable regulations
Travel Tracker Records	2 years or based on contractual commitments	3 years or based on contractual commitments
Other Records	2 years or based on applicable regulations	2 years or based on applicable regulations

Refer "West Bengal State Electronic Data Centre Storage Sharing and Electronic Data Retention Guidelines, 2020" for details.

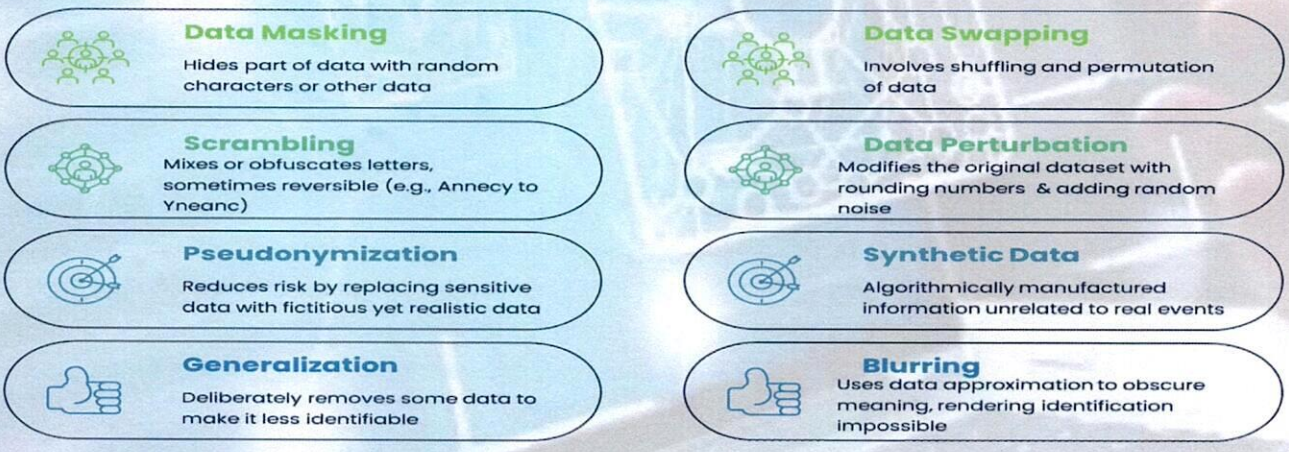
DATA ANONYMIZATION

What is data anonymization?

Data anonymization is a process that involves transforming or altering personal identifiers (Personally Identifiable Information) from a dataset to protect individuals' privacy and identity while preserving data utility. It involves techniques like removing explicit identifiers, aggregation, generalization, and adding noise to make re-identification difficult. The goal is to maintain data usefulness for analysis while safeguarding privacy, especially in compliance with data privacy regulations. Data anonymization is an integral part of data privacy.

Personally Identifiable Information (PII) refers to any data or information that can be used to identify a specific individual. PII includes personal data, such as names, addresses, social security numbers, Aadhaar card number, date and place of birth, mother's maiden name, PAN Card Number, email addresses, phone numbers, biometric data, and other information such as medical, educational, financial, and employment.

Different Anonymization Techniques commonly used are:



How to ensure data anonymization and adhere to data privacy?

- ✓ Data fiduciaries should ensure that an individual cannot be re-identified from their anonymized data
- ✓ Data fiduciaries should instruct the Data Processors and ensure that personal data is shared only in anonymized form
- ✓ Data fiduciaries should make strategies considering different industries and sectors having varied arrangements and models that can be used for sharing anonymized data

Refer "West Bengal State Public Transactional Data Sharing Guidelines, 2020" for details.

EXEMPTIONS

There are certain scenarios under which Data Principals do not possess the right to request erasure, correction, access to their personal data, or withdraw their consent. The scenarios are given below:

SCENARIO 01

For notified agencies, in the interest of security, sovereignty, public order, etc

SCENARIO 02

For research, archiving or statistical purposes

SCENARIO 03

For medical emergencies, employment

SCENARIO 04

To enforce legal rights and claims

SCENARIO 05

To perform judicial or regulatory functions

SCENARIO 06

To prevent, detect, investigate or prosecute offences

SCENARIO 07

To process personal data of non-residents under foreign contract in India

SCENARIO 08

For approved merger, demerger etc

SCENARIO 09

To locate defaulters and their financial assets etc

RESOURCE CREATION AND CAPACITY BUILDING

RESOURCE CREATION

The Organizations or Government Bodies which will be designated as Significant Data Fiduciary should appoint a **Data Protection Officer** and an independent data auditor **(Data Protection Auditor)**.

DoS of the Data Protection Officer (DPO) is:

- ✓ Function as a representative of the Significant Data Fiduciary
- ✓ Be responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary
- ✓ Point of contact (POC) to address the Data Principals for the grievance redressal mechanism
- ✓ Respond to communications from Data Principal in case the Data Principal wishes to exercise his/her/its rights or raises any question or wants to access information about their personal data processing

DoS of the Data Protection Auditor (DPA) is:

- ✓ Conduct data audit
- ✓ Evaluate compliance of the Significant Data Fiduciary to various applicable laws, acts and regulations

CAPACITY BUILDING

To increase awareness and skills among the employees of the Government and other Organizations, it is required to conduct periodic training to sensitize them about their rights and duties and guidelines to prevent risk of being susceptible to breaches.

The training should encompass:

- ✓ General awareness programs for all employees to foster a culture of data privacy
- ✓ Specific departments, such as IT and Legal, will be trained on specialized modules of data privacy rules and their implementation
- ✓ Mandatory training topics including data security best practices, understanding and compliance with data privacy regulations, recognizing and responding to data breaches, and safeguarding personal and confidential information

IMPLEMENTATION FRAMEWORK

West Bengal Electronics Industry Development Corporation Limited will be nominated as the State Implementing Agency (SIA) and State Level Nodal Agency (SLNA) for advising, training, and promoting data privacy within the State of West Bengal.

WBEIDC Ltd will be responsible for the advising, training, and promoting data privacy concept and its guidelines to different Government bodies ULBS, Corporations, Development Authorities, District, Sub-Divisions, Blocks, Gram Panchayats, etc. across the State of West Bengal including private organizations. District level sensitization programs will be conducted by this vertical and other domain experts.

THANK YOU

DOCUMENT OWNER

Shri Sanjay Kumar Das,
Additional Secretary

Dept of IT & Electronics, Govt of West Bengal,
Webel Bhawan Complex, Moni Bhandar,
Block EP & GP, Sector- V, Salt Lake, Kolkata-700091

Email: adlsit@wb.gov.in