INDIVIDUAL DATA ACCESS & SHARING *PROTECTION POLICY*

DEFINITION & CASE STUDY IN BANK INDONESIA

ROME, OCTOBER 18, 2023

1 BACKGROUND:
CHALLENGES & URGENCY

Challenges in Global & National Environment

01 *Global Digitalization Megatrend*
Creating opportunities to accelerate access, activities that further increase connectivity and change business processes in various sectors.

02 *Data Protection Regulatory Basis*
Indonesia has passed Personal Data Protection Law and Law on Developing and Strengthening Financial Sector as commitment to protect confidential data

03 *Data Breach Cases*
Statista reports that 66% of organizations worldwide were victim of ransomware attacks between March 2022 and March 2023.

04 *Granular Data Need in Policy-Making*
The dynamics of macroeconomic and financial market pressures have led to an increase in the need for granular data as a basis for policy making.

Impact toward Organization's Business Process

Fast Access & Sharing on Individual Data

vs.

Individual Data Protection

2

1 PROBLEM STATEMENT

1) **Why** should we **protect individual data?**
2) **How** can we protect the individual data in terms of **access and sharing arrangement?**

2

INDIVIDUAL DATA CONCEPT

Why do We Need to Protect Individual Data?

INDIVIDUAL DATA

Covering Personal and Single Organizational Data

*'**Individual Data**' refers to…*

1. *natural person (human) and/or*
2. *single entity of corporate data (data subject)*
3. *due to its confidential nature or having non-disclosure right*

Risk of Individual Data Disclosure

Legal

- ❑ **Non-compliance** with data protection laws
- ❑ **Lawsuit** filed by disadvantaged party

Financial

- ❑ Paying ransom for data theft by hacker
- ❑ Paying compensation due to legal claims

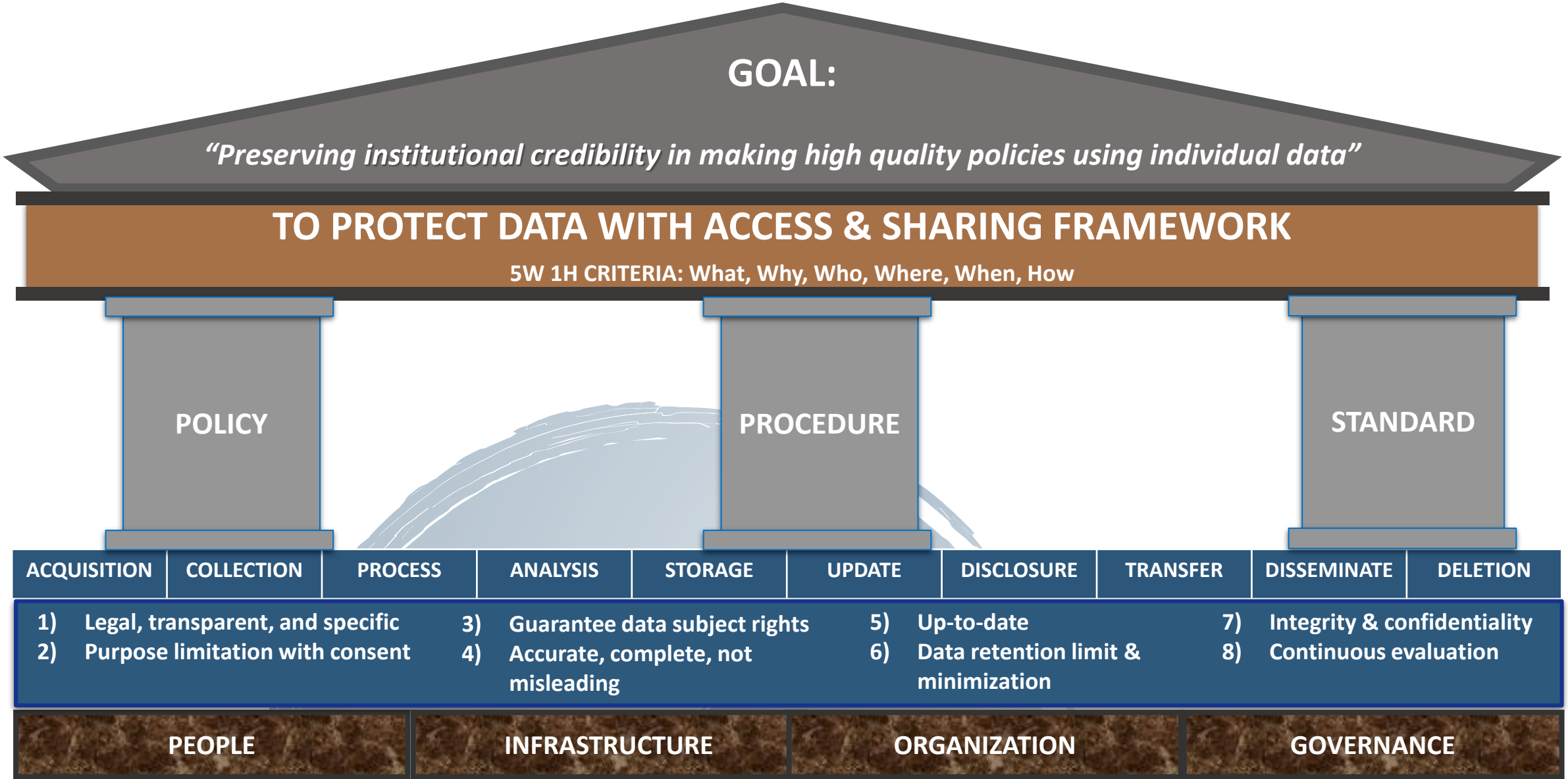
Reputation

- ❑ Damage to public trust
- ❑ May defect policy credibility

3

DATA ACCESS FRAMEWORK:

DATA ACCESS CONTROL BY DESIGN



4a DATA ACCESS FRAMEWORK:
ACCESS PROTECTION CRITERIA – (5W1H APPROACH)

What

1. Data/Information
2. Applications or system

Why

User should inform **the objective** and **the legal basis** for requesting access.

The basis for the provisions:
(1) National law,
(2) Internal regulation,
(3) Executive level decisions, and
(4) Other legitimate interests (e.g. MoU, and International Standards)

Who

Categories of standardized user who are eligible to be given access:
1. Data User
2. Application Operator
3. Data Contributor
4. Infrastructure Administrator
5. Supervisor
6. Legitimate External Stakeholders

Where

The Access channel may consist of:
(i) On-Premise Application,
(ii) Internal Communication Platform,
(iii) Cloud Sharing Access,
(iv) Visualization Tools.

When

1. Access must be provided depending on the **characteristics**, **urgency** and **risks** of providing access to the data/application.
2. Retention period:
   - **Minimum 1 month**
   - **Maximum 1 year**
3. Can be **ad hoc** or on **regular basis.**

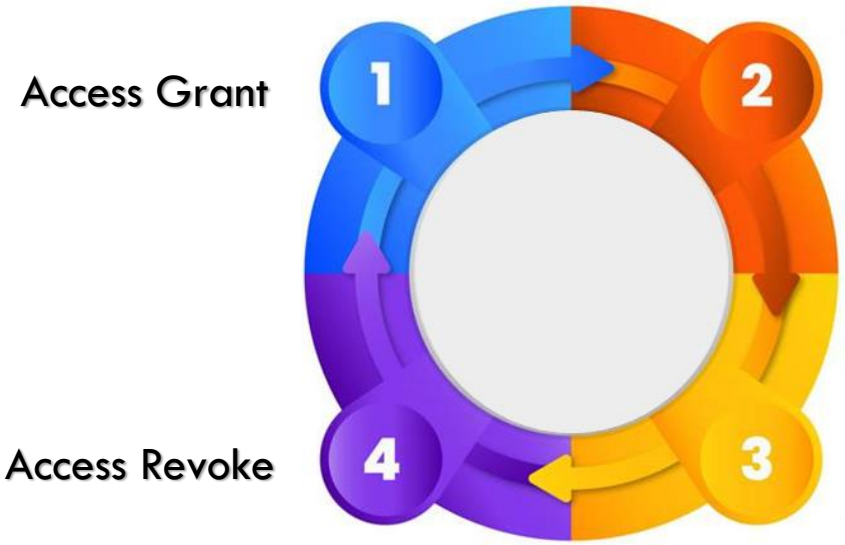
How

- Define a centralized data governance committee focus on individual data access and data sharing.
- Implementing **3-layer decentralized accountability commitment** for:
  1. Data user of a department,
  2. Information manager on the department,
  3. Head of department.

4b

DATA ACCESS FRAMEWORK:
LIFE CYCLE & INSTITUTIONAL ARRANGEMENT

ACCESS LIFECYCLE



1. **Access Grant:** the process of granting new access submitted by prospective users by completing the mandatory procedures**.**
2. **Access Usage:** the period of access usage by approved users for the specific set of time**.**
3. **Access Period Extension:** the process of extending an access retention period due to expiry.
4. **Access Revoke:** the process of revoking a user's access.

INSTITUTIONAL ARRANGEMENT

DATA CONTRI-BUTOR

DATA PRODUCER

DATA APLICATION ADMIN

Coordinator of Information Managers

DATA GOVERNANCE COMMITTEE

Access to Internal Data User

Dept. Head A	*Dept. Head B*
Information Manager	*Information Manager*
User A.1 User A.2 . . .	User B.1 User B.2 . . .

Sharing to External Parties

Individual Person

Private Organization

International Body

4C

DATA ACCESS FRAMEWORK:
ACCESS RESPONSIBILITY MATRIX (RACI)

	Head of Department	*Information Manager*	*Internal Data User*
Access Request	**RESPONSIBLE, ACCOUNTABLE**	**RESPONSIBLE, CONSULT**	**RESPONSIBLE**
Data Usage	**ACCOUNTABLE, INFORMED**	**INFORMED**	**RESPONSIBLE**
Data Sharing	**ACCOUNTABLE**	**CONSULTED**	**RESPONSIBLE**

5 FINAL WRAP-UP:
CONCLUSION & KEY TAKE AWAYS

Needs of Individual Data in Central Bank
Central banks nowadays dive deeper into microdata utilization to produce accurate & up-to-date policy.

Need to Protect Individual Data
The global issue of data breach and the concern of protecting private data becomes high priority.

Data Protection by Access Control Policy
Governing data access and sharing is very important because human aspect is the most vulnerable.

KEY TAKE AWAYS

1. The balance between processing individual data for good policy-making and protecting the data can be achieved by implementing a good data protection framework.

2. A good data access protection framework should define purpose clarity, strategies, and guiding principles.

3. Data Access & Sharing Protection Framework consist of:
   a. Data **Access Protection Criteria**.
   b. Data **Access Lifecycle & Institutional Arrangement**.
   c. Data **Access Responsibility Matrix**.

4. Organizational structure should have a centralized data governance committee that bridges data producer/contributor and the data user.

BANK INDONESIA
BANK SENTRAL REPUBLIK INDONESIA

ANY QUESTION?

Author:

- Johanes Iman Anugrah
- Akhmad Zacky Nugraha
- Sapto Widyatmiko

"Data Should Be Protected Like Our Bodies"