IFC-Bank of Italy Workshop on "Data science in central banking: enhancing the access to and sharing of data"

17-19 October 2023

Individual data access and sharing protection policy: definition and case study of Bank Indonesia[1]

Johanes Iman Anugrah, Akhmad Zacky Nugraha and Sapto Widyatmiko,
Bank Indonesia

[1] This contribution was prepared for the workshop. The views expressed are those of the authors and do not necessarily reflect the views of the Bank of Italy, the BIS, the IFC or the other central banks and institutions represented at the event.

Individual Data Access & Sharing Protection Policy

Definition and Case Study of Bank Indonesia

Johanes Iman Anugrah, Akhmad Zacky Nugraha, Sapto Widyatmiko

Abstract

The information age presents a fundamental paradox: the unprecedented potential for data-driven progress stands in stark contrast to growing concerns about individual privacy and security. Navigating this tightrope, where efficient access and exchange clash with fundamental rights, demands a robust "Individual Data Access & Sharing Protection Policy" (IDASP). This paper explores the intricacies of IDASP, examining its goals, principles, and practical implementation frameworks.

We begin by outlining the pressing need for data protection in the digital era, highlighting both the benefits of information exchange and the vulnerabilities it exposes. We then delve into the theoretical underpinnings of IDASP, defining "individual data" and exploring the rationale behind its protection. This includes safeguarding personal information, maintaining confidentiality of sensitive corporate data, and upholding fundamental principles like privacy, trust, and accountability.

The core of the paper examines the practical aspects of IDASP implementation. We present a comprehensive data access control framework built on the "5W1H" approach, addressing crucial questions about what data is protected, why access is granted, who can access it, where and when they can access it, and how the process is governed. This framework emphasizes granular control, purpose limitation, robust security measures, and transparency throughout the "Access Life Cycle," encompassing pre-access onboarding, monitored usage, cautious extensions, and swift revocation mechanisms.

Furthermore, we discuss the essential role of the Access Responsibility Matrix (RACI) in defining clear roles and responsibilities for data access and sharing within an organization. This ensures accountability at all levels, promotes responsible data handling, and fosters trust in data governance practices.

This paper argues that IDASP is not merely a regulatory checkbox, but a strategic imperative for navigating the data-driven future with responsibility and integrity. By prioritizing individual control, responsible data utilization, and transparent governance, IDASP empowers organizations to leverage the power of information while preserving trust and building a data-driven world where both individuals and organizations can thrive.

Keywords: Individual data privacy, data protection, data governance, IDASP, data access control, data sharing.

Contents

Introduction/Background

The data-driven age presents a paradox: the unprecedented potential for information exchange and societal progress stands in stark contrast to the mounting concerns regarding individual data privacy and security. As the global digital landscape expands, blurring geographical boundaries and transforming business processes across sectors, the need for a robust "Individual Data Access & Sharing Protection Policy" (IDASP) becomes increasingly urgent.

On the one hand, global digitalization fuels an interconnected world, fostering faster access to information and resources. This megatrend unlocks unparalleled opportunities for businesses, facilitating streamlined operations, personalized experiences, and innovative products. For governments, granular data can inform evidence-based policymaking, driving economic growth and social welfare. Yet, this very interconnectedness breeds vulnerabilities.

Indonesia's commitment to data protection, exemplified by its latest Personal Data Protection Law and the Financial Sector Development and Reinforcement Law, highlights the growing recognition of this imperative. However, real-world challenges cast a shadow on this commitment. Statista's report in 2022 has revealed that numbers of global organizations became the victim to ransomware attacks in just a year, which serves as a stark reminder of the ever-present threat of data breaches.

Further complicating the issue is the inherent tension between rapid data sharing and individual protection. Businesses thrive on efficient access to and exchange of customer information, often seeking faster processing and streamlined data flows. Yet, these very processes raise concerns about potential misuse, unauthorized access, and the erosion of individual control over personal data. This dichotomy, where process efficiency clashes with privacy rights, lies at the heart of the IDASP dilemma.

Navigating this crossroads demands a nuanced approach. We must find ways to unlock the benefits of data exchange while ensuring robust safeguards for individual privacy. The urgency for a comprehensive IDASP lies not only in mitigating the risks of data breaches and safeguarding fundamental rights, but also in fostering trust and confidence in the digital ecosystem. It is time to bridge the gap between the imperatives of access and protection, paving the way for a future where both individuals and organizations can flourish in the data-driven age.

Problem Statement

In the digital age, individual data has become a valuable commodity, constantly collected, accessed, and shared across the web. While this interconnectedness offers undeniable benefits, it also raises two critical questions: why should we protect individual data, and how can we ensure its security in the face of ubiquitous access and sharing?

Finding solutions to these challenges requires a multi-pronged approach involving individuals, businesses, governments, and civil society. Embracing a comprehensive IDASP framework that prioritizes informed consent, granular control, and robust

security measures is the first step towards building a future where both data sharing and individual data protection can thrive.

Theoretical Basis

The concept of "Individual Data" encompasses a fundamental element of our digital age: the need to protect the information that defines and belongs to individual entities. This theory will explore the "why" and "what" of individual data protection, considering both personal data and certain corporate data falling under this umbrella.

2.1. Defining Individual Data:

Based on our cases, we define the term "individual data" as:

- Natural Persons (Humans): This includes any data directly or indirectly identifiable with a specific person, such as name, address, financial records, health information, biometric data, and online activity, as referred in Indonesia's Personal Data Protection Law as well as GDPR.
- Single Entity of Corporate Data (Data Subject): In certain contexts, specific corporate data can be considered "individual" if it relates to a single identifiable entity within the organization and possesses confidential or non-disclosure characteristics. This could include intellectual property, trade secrets, or sensitive financial information, or any other non-public information that could potentially cause legal, financial, or even reputational risks to the data controller or processor.

2.2. The Necessity of Individual Data Protection:

Protecting individual data transcends mere legal compliance. It's driven by fundamental principles and essential considerations, as also described in different perspective in following framework diagram in section 3.1:

1. Privacy and Autonomy: Protecting personal data safeguards individuals' right to privacy and control over their personal information. This includes preventing unauthorized access, discrimination based on personal data, and the ability to choose how and when their information is shared.
2. Confidentiality and Non-Disclosure: Certain corporate data, even though not directly tied to a specific person, can hold significant confidential or non-disclosure value. Protecting this "individual" data ensures fair competition, prevents intellectual property theft, and safeguards sensitive financial information.
3. Security and Risk Mitigation: Data breaches and unauthorized access can have devastating consequences for both individuals and organizations. Robust data protection measures minimize these risks and safeguard sensitive information.

4. Accountability and Trust: Building trust in the digital ecosystem requires transparency and accountability in data handling practices. Effective protection frameworks ensure responsible data use and empower individuals to hold organizations accountable for breaches or misuse.

Implementing effective protection measures requires a multi-layered approach:

- Granular Access Control: Individuals and organizations should have control over who accesses their data, for what purposes, and for how long. This can involve opt-in/opt-out mechanisms, tiered access levels, and detailed audit logs.
- Data Minimization and Purpose Limitation: Collecting and sharing only the minimum necessary data for specific purposes reduces the risk of exposure and misuse. Clear purpose justification and limitations on secondary data use are crucial.
- Security and Encryption: Implementing robust security measures like encryption, regular backups, and vulnerability assessments is essential to protect data from unauthorized access, loss, or alteration.
- Transparency and Accountability: Organizations handling individual data must be transparent about their practices, inform data subjects about collection and sharing, and be held accountable for breaches or misuse. Clear privacy policies, regular audits, and effective redress mechanisms are key.

The concept of "Individual Data" encompasses both personal and certain corporate data requiring protection due to its confidential nature or non-disclosure right. Recognizing the significance of individual data protection and implementing effective safeguards is crucial to upholding fundamental rights, building trust in the digital ecosystem, and fostering responsible data practices in our data-driven world.

2.3. Risk of Individual Data Disclosure

In today's interconnected world, individual data sits at the heart of countless transactions, interactions, and operations. Unfortunately, the ease of access and sharing often obscures the inherent risks associated with data disclosure. A robust "Individual Data Access & Sharing Protection Policy" (IDASP) acts as a vital shield, minimizing these risks and safeguarding the very fabric of digital trust.

Failing to uphold an effective IDASP exposes organizations to a trio of perilous consequences:

1. Legal Loss:

- Non-Compliance with Data Protection Laws: Breaches of IDASP principles can trigger hefty fines and penalties under relevant data protection regulations. Indonesia's Personal Data Protection Law and Law on Financial Sector

Development and Reinforcement stand as reminders of the legal ramifications of data security lapses.

- Lawsuits and Damages: Disadvantaged parties – individuals whose data has been compromised due to IDASP failure – have the right to seek legal recourse. This can translate into costly lawsuits and compensation claims, draining both financial resources and reputation.

2. Financial Fallout:

- Ransomware Woes: Data breaches perpetrated by malicious actors often lead to ransom demands, forcing organizations to fork over hefty sums to regain control of their sensitive information. The financial impact of such cyberattacks can be crippling, disrupting operations, and impacting profitability.
- Compensation Claims: Legal claims arising from data breaches and IDASP non-compliance can lead to significant financial burdens. Compensation awarded to affected individuals can drain resources and impact an organization's bottom line.

3. Reputational Ruin:

- Public Trust Erosion: When individual data is compromised, the organization responsible faces a steep decline in public trust. Consumers become wary, stakeholders express concern, and the brand image suffers irreparable damage. Rebuilding trust becomes a long and arduous process.
- Policy Credibility Collapse: An IDASP framework that fails to protect individual data effectively becomes hollow and ineffective. Its credibility plummets, rendering it useless in safeguarding sensitive information and fostering responsible data practices within the organization.

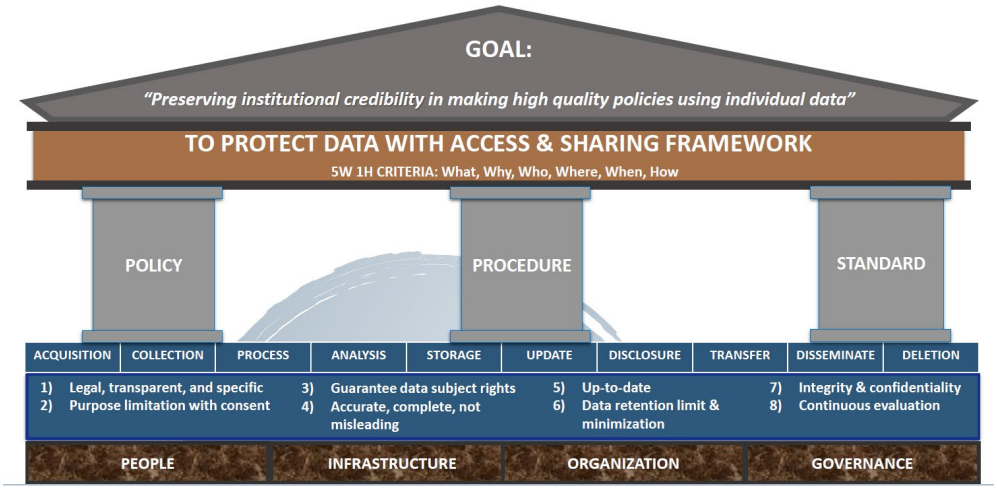
These risks highlight the critical importance of an effective IDASP. It is not merely a regulatory checkbox; it is a vital investment in protecting the organization, its stakeholders, and ultimately, the very foundation of trust in the digital ecosystem. By prioritizing robust data security measures, granular access control, and unwavering transparency, organizations can mitigate these risks and navigate the data-driven world with confidence and responsibility.

The peril of individual data disclosure in the absence of a strong IDASP cannot be overstated. The legal, financial, and reputational repercussions can be far-reaching and devastating. Embracing and effectively implementing an IDASP framework is not just a legal requirement; it is a strategic imperative for navigating the digital age with prudence and integrity.

Methodology and Data Framework

Based on the principles that we defined before, we propose a protection framework particularly in data access arrangement, which will be elaborated in this section.

3.1. Data Access Control by Design



The cornerstone of a robust "Individual Data Access & Sharing Protection Policy" (IDASP) lies in its data access framework. This framework, aptly named "Data Access Control by Design," aims to transcend mere data security by ensuring the preservation of institutional credibility in making high-quality policies based on accurate and responsibly accessed individual data.

3.1.1. Protecting Data with the 5W1H of Access

The framework operates on the principle of providing clear and granular control over data access, addressing the crucial questions of:

- What: All individual data and applications/systems used for processing, storing, or accessing it.
- Why: Users must state their objective and legal basis for access, ensuring data is used only for legitimate purposes.
- Who: Predefined user categories with specific privileges (data users, operators, contributors, etc.).
- Where: Permitted access channels like on-premise applications, internal platforms, cloud sharing, and visualization tools.
- When: Access duration based on data characteristics, urgency, and risks, with minimum of 1 month, maximum of 1 year, and possibility of ad hoc or ongoing access.
- How: A centralized Data Governance Committee oversees access, supported by a three-layer decentralized accountability system within departments.

3.1.2. Embedded in Policy, Procedure, and Standard

The Data Access Control framework is integrated into three key governance elements:

- Policy: Clearly defines objectives, principles, and user categories for data access.

- Procedure: Outlines specific steps for requesting, granting, and monitoring access rights.
- Standard: Establishes technical and security protocols for secure data access and exchange.

3.1.3. Guidance for Responsible Data Handling

This comprehensive framework is further strengthened by applying eight key guidance principles, embedded within policy, procedure, and standard:

- Legal, transparent, and specific: Access aligns with data protection laws, is processed in transparent manner to data subjects, and specifies user roles and purposes.
- Purpose limitation with consent: Access is granted only for documented purposes with informed consent from data subjects whenever necessary.
- Guarantee data subject rights: Individuals have the right to access, rectify, erase, and restrict processing of their data.
- Accurate, complete, not misleading: Data used for policymaking must be accurate, complete, and not misleading.
- Up to date: Regular data updates ensure accuracy and reliability.
- Data retention limit & minimization: Data is retained only for the minimum necessary period and then securely disposed off.
- Integrity & confidentiality: Robust security measures protect data from unauthorized access, alteration, or loss.
- Continuous evaluation: Regular framework review and updates adapt to evolving needs and regulations.

3.1.4. The Power of Collaborative Governance

Effective data access control necessitates the involvement of various entities:

- People: Individuals responsible for data access and policy implementation must be adequately trained and accountable.
- Infrastructure: Secure IT systems and infrastructure are essential for data storage and transmission protection.
- Organization: Establishing a data governance structure within the organization ensures clear lines of responsibility and oversight.
- Governance: Regular audits, assessments, and effective redress mechanisms strengthen the overall data governance framework.

By integrating these elements, the Data Access Control by Design framework fosters a culture of responsible data stewardship and builds trust with individuals. This, in turn, empowers the organization to make informed policy decisions based on accurate and secure individual data, preserving institutional credibility, and fostering continued success in the data-driven era.

3.2. Access Protection Criteria – (5W1H Approach)

This framework empowers individuals with control over their data while enabling responsible data use within the organization. It ensures transparency and trust by clearly defining:

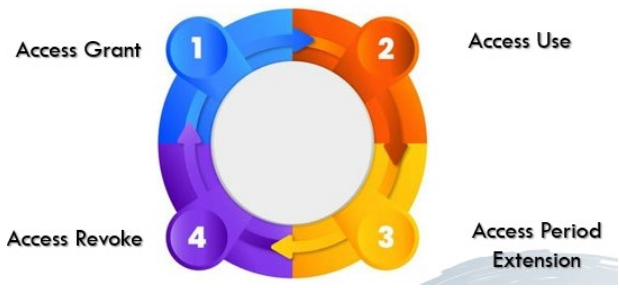
- What: All individual data and applications/systems used for processing, storing, or accessing it.
- Why: Users must state their objective and legal basis for access, ensuring data is used only for legitimate purposes.
- Who: Predefined user categories with specific privileges (data users, operators, contributors, etc.).
- Where: Permitted access channels like on-premise applications, internal platforms, cloud storage sharing, and visualization tools.
- When: Access duration based on data characteristics, urgency, and risks, with minimum of 1 month, maximum of 1 year, and possibility of ad hoc or ongoing access.
- How: A centralized Data Governance Committee oversees access, supported by a three-layer decentralized accountability system within departments.

This comprehensive framework protects individual data, builds trust, and fosters responsible data utilization within the organization. Apart from these criteria, there are still several considerations that will be added to the framework, this will strengthen the previous criteria, including:

- The framework emphasizes legal compliance and internal regulations for data access.
- Access is granted based on legitimate interests and external agreements.
- Anonymization and aggregation techniques can be used for data visualization.
- Regular review and updates ensure the framework adapts to evolving needs.

This comprehensive framework addresses the 5W1H of data access, empowering individuals with control over their data while enabling responsible data utilization for legitimate purposes. By implementing this framework, the organization fosters a culture of data privacy and builds trust with all stakeholders.

3.3. Access Life Cycle



The "Individual Data Access & Sharing Protection Policy" (IDASP) ensures continuous control and oversight over individual data access through a comprehensive "Access Life Cycle." This cycle encompasses four stages:

1. Access Grant: Stringent On-boarding
    - Rigorous identity verification confirms user eligibility and authorized roles.
    - Users articulate clear and documented purpose for requiring access.
    - Mandatory training equips users with data protection and responsible handling practices.
    - A thorough risk assessment evaluates potential issues associated with granting access.
2. Access Usage: Monitored Activity
    - Detailed logs track all user access attempts, data accessed, and actions performed.
    - Time-bound access minimizes exposure and prevents unnecessary data contact.
    - Automatic notifications warn users and administrators of approaching expiry.
    - Close monitoring ensures adherence to the approved purpose and prevents misuse.
3. Access Period Extension: A Cautious Approach
    - Extensions require a compelling justification and renewed purpose statement.
    - A thorough re-assessment of risks and potential impacts is conducted.
    - Approval requires authorization from relevant data governance parties.
4. Access Revoke: Swift and Decisive Action
    - Data subjects have the right to request access revocation under specific circumstances.
    - Security breaches or misuse by users trigger immediate access revocation.
    - Changes in user roles or status may necessitate access modification or revocation.

This cycle prioritizes individual control, responsible data utilization, and transparent monitoring. It safeguards sensitive information throughout its journey, building trust and fostering data security within the organization.

The Access Life Cycle within the IDASP framework emphasizes a proactive and vigilant approach to protecting individual data. By incorporating stringent onboarding procedures, continuous monitoring, and a well-defined process for access extension and revocation, the IDASP safeguards sensitive information

throughout its journey, upholding individual privacy and building trust in the organization's data handling practices.

3.4. Access Responsibility Matrix (RACI)

A robust "Individual Data Access & Sharing Protection Policy" (IDASP) requires not only comprehensive frameworks but also clear lines of responsibility. This is where the Access Responsibility Matrix (RACI) comes into play, delineating roles and ensuring accountability throughout the data lifecycle.

3.4.1. The RACI Matrix in Action

This matrix outlines who is Responsible, Accountable, Consulted, or Informed (RACI) for various aspects of data access and sharing within the organization. Let's delve into the specific roles for each stage:

1. Access Request:
    - Head of Department (HoD): Ultimately responsible and accountable for approving access requests, ensuring alignment with data protection regulations and departmental needs.
    - Information Manager (IM): Responsible for providing consultation and advice to the HoD during review, assessing potential risks and recommending appropriate access levels.
    - Internal Data User (IDU): Responsible for submitting clear and justified access requests, specifying purpose and legal basis for data utilization.
2. Data Usage:
    - Head of Department (HoD): Accountable for overall data usage within their department, staying informed about how data is being utilized and ensuring adherence to approved purposes.
    - Information Manager (IM): Informed about data usage patterns, identifying potential discrepancies or misuse and notifying the HoD if necessary.
    - Internal Data User (IDU): Responsible for using data only for approved purposes, upholding data protection regulations, and reporting any irregularities.
3. Data Sharing:
    - Head of Department (HoD): Accountable for all data sharing activities within their department, authorizing only legitimate and secure sharing practices.
    - Information Manager (IM): Consulted on data sharing decisions, providing guidance on secure sharing methods and potential compliance risks.
    - Internal Data User (IDU): Responsible for sharing data only in accordance with approved purposes and established protocols, ensuring recipient authorization and secure transmission.

3.4.2. Benefits of the Access Control RACI Matrix

The RACI matrix offers several advantages for the IDASP:

- Clear Delegation of Responsibility: Clearly defined roles prevent confusion and ambiguity, ensuring everyone knows who is accountable for each stage.
- Enhanced Accountability: Holding individuals accountable for their actions fosters responsible data handling and minimizes the risk of misuse.
- Improved Communication: The matrix facilitates communication between departments and roles, enabling streamlined workflow and efficient handling of data access and sharing requests.
- Strengthened Trust: By ensuring transparent and responsible data governance, the RACI matrix builds trust with individuals and stakeholders.

The RACI matrix is an invaluable tool for implementing and upholding the IDASP. By clearly defining roles and responsibilities, it fosters accountability, promotes responsible data handling, and ultimately builds trust in the organization's data governance practices.

Conclusion and Key Take Aways

Overall, the IDASP framework provides a valuable roadmap for organizations navigating the complex world of data access and sharing in the digital age. By embracing its principles and implementing its measures, organizations can protect individual data, build trust, and thrive in the data-driven future.

4.1. Conclusion

- 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.

The IDASP framework offers a comprehensive approach to protecting individual data in the digital age. By prioritizing individual control, responsible data use, and transparent monitoring, it fosters trust and minimizes risks associated with data access and sharing. Implementing this framework empowers organizations to leverage the benefits of data while upholding fundamental privacy rights and building trust with stakeholders.

4.2. Key Takeaways:

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.

References

D. Garcia, E. Fernandez, F. Lopez (2022): "The RACI Model: A Practical Approach to Data Protection Accountability", International Journal of Law and Information Technology.

Earley, S., Henderson, D., Sebastian-Coleman, L. (2017): "The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK)", DAMA International.

European Union (2018): General Data Protection Legislation.

Indonesia (2022): National Legislation on Personal Data Protection.

Indonesia (2023): National Legislation on Financial Sector Development and Reinforcement.

Nils Gruschka, Vasileios Mavroeidis, Kamer Vishi and Meiko Jensen (2018): "Privacy issues and data protection in big data: A case study analysis under GDPR", IEEE International Conference on Big Data Big Data 2018, pp. 5027-5033, December.

Stalla-Bourdillon S, Thuermer G, Walker J, Carmichael L, Simperl E (2020): "Data protection by design: Building the foundations of trustworthy data sharing. Data & Policy", Cambridge Press.

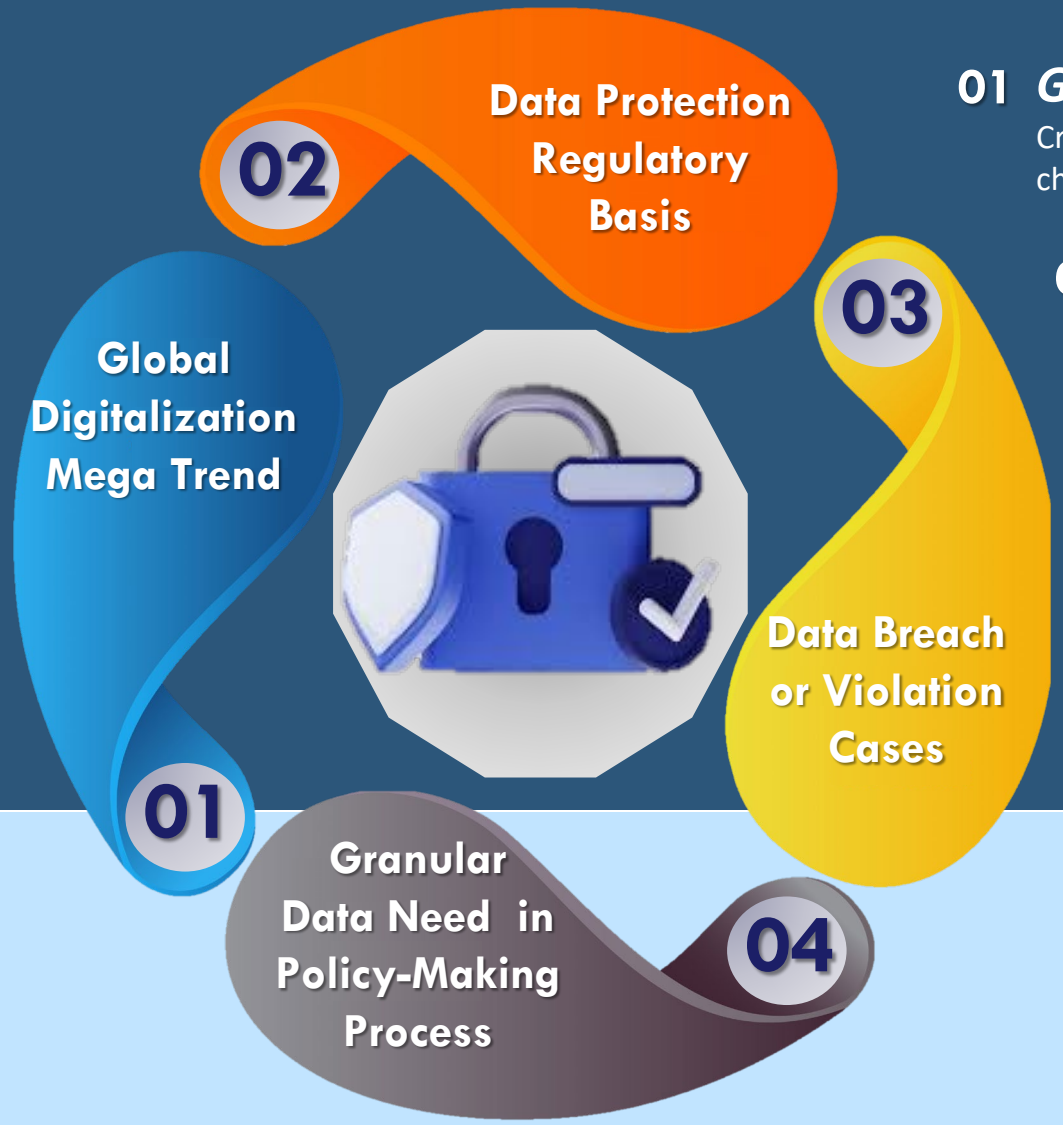
Tiwari S, Sharma S, Shetty S, Packer F. (2022): "The Design of a Data Governance System", BIS Paper, no. 124, May.

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?**

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

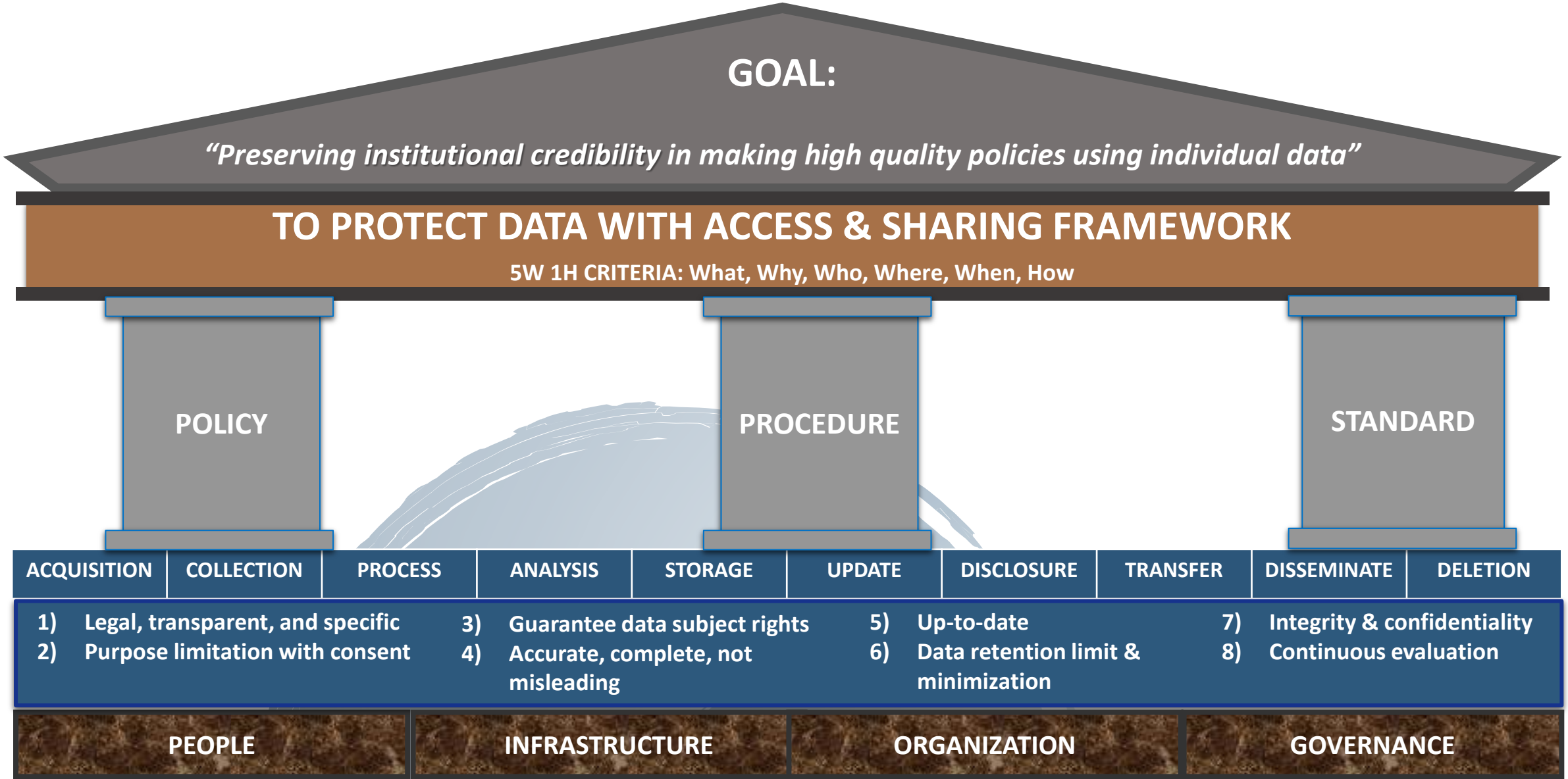
Reputation

- ❑ 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.**

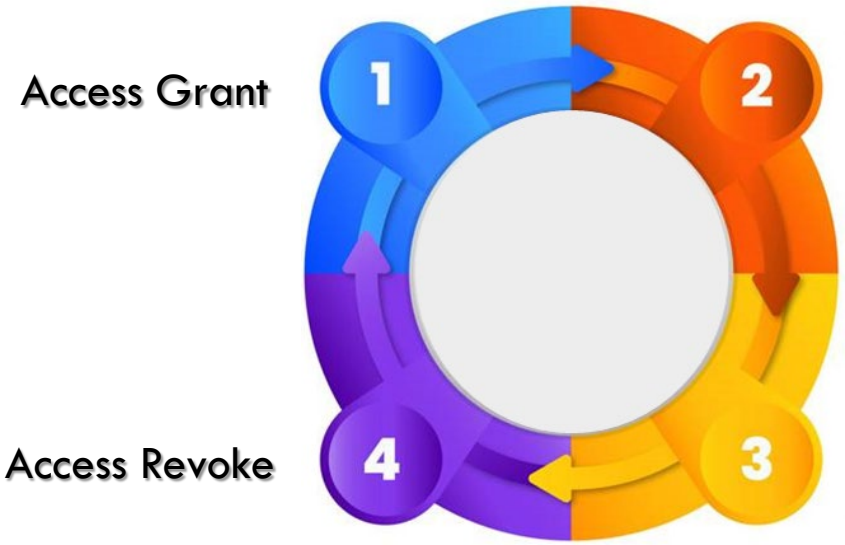
How

- 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"