smeru
RESEARCH INSTITUTE

Toward Pro-Poor Policy through Research

POLICY ON

PROTECTION OF PERSONAL DATA

The SMERU Research Institute
7 December 2022

POLICY ON PROTECTION OF PERSONAL DATA

Developed by/ Version submitted for approval/ Date of Submission	Institute Secretary/ First version (v.2)/ 2 December 2021	
Approved by/ Date approved	Director/ 7 December 2022	
Effective date	1 January 2023	
Acknowledgement by Responsible Departments	Information Technology Section	
	Research Department	
	Human Resources & General Affairs Department	
	Publication Department	
Review of policy implementation due	7 December 2025 -	

Table of Contents

1. Background and Purpose

SMERU is committed to respecting the privacy of individuals and ensuring that any information collected, stored, used or otherwise processed by SMERU is done so in accordance with Indonesia's regulation and recognized international practices and standards. In order to adequately protect the personal data of all individuals, including SMERU staff, service providers, applicants, individuals and corporations involved in SMERU's programmatic activities or outreach, while at the same time ensuring that SMERU can carry out its programs and efficiently execute required administrative actions, the Policy on Protection of Personal Data (the "**Policy**") set out the requirements to be followed by SMERU when handling personal data.

This Policy applies to Personal Data processed by SMERU. It applies to all staff members of SMERU, consultants, contractors, interns, volunteers, secondees, or other SMERU stakeholders, regardless of location, to the extent that they are Controlling or Processing Personal Data under the name of SMERU as a Data Controller or Data Processor with respect to Personal Data relating to Data Subjects.

2. Definitions

The following definitions apply for the purpose of this Policy:

"Data Subject" includes all living individuals about whom SMERU holds personal data. A data subject includes any individual person or corporate who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, mental, economic, cultural, or social identity.

"Consent" means any freely given informed indication of an agreement by a Data Subject to the Processing of his or her Personal Data, which may be given by a written or oral statement or by a clear affirmative action;

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

"Data Controller" means the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed;

"Data Transfer" or "Transfer" means any act that makes Personal Data accessible, whether on paper, via electronic means or any other method, to a third party;

"Personal Data" shall mean any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Processing" means any operation which is performed involving Personal Data such as collection, recording, organization, structuring storage adaptation or alteration, use, disclosure, restriction, erasure, or destruction;

"Processor" means the natural or legal person which processes Personal Data on behalf of the Data Controller; and

"Sensitive Personal Data" means Personal Data revealing racial or ethnic origins, political opinions, trade union membership, religious or philosophical beliefs, health, or sexual life, genetic or biometric data, or criminal convictions of a Data Subject. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3. Principles relating to Processing Personal Data

SMERU, as Data Controller or Processor, shall be guided by the following principles in relation to all actions relating to Personal Data.
Personal Data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

b) Collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;

d) Accurate and where necessary, kept up to date;

e) Kept in a form which permits identification of Data Subjects for no longer than necessary for the purposes for which the data are Processed; and

f) Processed in a manner which ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage using appropriate technical or organizational measures.

4. Purpose for Processing of Personal Data

4.1 Any Processing of Personal Data should be proportionate to the purpose for which it is being Processed. The Personal Data collected and processed should be adequate and relevant for the identified purpose and should not exceed that purpose (legitimate ground).

4.2 SMERU as Data Controller shall ensure that Personal Data shall be processed only if and to the extent at least one of the following applies:

a) The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes;

b) Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps necessary prior to entering into a contract;

c) Processing is necessary for compliance with a legal obligation to which the Data Controller is subject, including compliance with SMERU's legal framework;

d) Processing is necessary to protect the vital interest of the Data Subject or another natural person;

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the authority vested in SMERU; or

f) Processing is necessary for the purpose of the legitimate interests pursued by SMERU or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the Data Subject which require protection of the Personal Data.

4.3 Processing of Sensitive Personal Data is not allowed, unless:

a) the Data Subject has given Consent;

b) the data have been made public by the Data Subject;

c) it is necessary to protect vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;

d) it is necessary to carry out investigative procedures; or

e) it is necessary to carry out obligations under the SMERU's Regulations and Rules, including those relating to health and social care.

4.4 Consent Management

a) SMERU will consider Consent as a legal basis for Processing only when Data Subjects have been informed about the Processing of their Personal Data.

b) When SMERU is relying on Consent as legal basis for Processing Personal Data, SMERU personnel processing the Personal Data must clearly establish the Data Subject's Consent and monitor Consent usage. Consent can be obtained in writing or electronically and is valid only if given voluntarily. To establish Consent, there should be a positive opt in (no pre-ticked boxes or default consent) by the Data Subject. SMERU personnel shall keep a record of when and how it obtained Consent, together with the Personal Data.

c) Data Subjects shall be provided with the possibility to withdraw their Consent at any time.

5. Data Processing by Third Parties

SMERU may Transfer Personal Data to third parties only on the following conditions:

a) The Data Subject is informed of the possible Data Transfer that is known when data is collected. The Transfer of Personal Data will be based on the requirements of the Statistic Law.;

b) The third party, as Processor, ensures data protection on at least the same level as SMERU and such level of data protection is established by a contract or other legally binding documentation;

c) The Data Transfer is made for one more or more legitimate purposes, as set out in paragraph 4 above; and

d) The amount of Personal Data transferred is strictly restricted to the data the third party needs to have for the specific purpose the third party receives the data.

6. Information to be provided

6.1 At the time the Personal Data is obtained, SMERU shall provide the Data Subject the following information:

a) SMERU's contact details;

b) The type of Personal Data related to the Data Subject Processed by SMERU;

c) The purposes of the Processing;

d) Legal basis for the Processing;

e) The recipient or categories of recipients (third parties) that the Personal Data are to be disclosed to, if the recipient is known before data is collected;

f) The period for which the Personal Data will be stored; and

g) How to exercise the Data Subject's rights set out in Section 7.

7. Rights of Data Subject

7.1 Right to Access. The Data Subject has the right to obtain confirmation as to whether Personal Data relating to the Data Subject has been collected, stored or processed, and, where that is the case, how the Personal Data was collected and processed and for what purpose, and to have access to copies of such Personal Data.

7.2 Right to Rectification. The Data Subject has the right to request rectification of Personal Data relating to the Data Subject if such data can be established to be inaccurate or incomplete.

7.3 Right to Erasure and Restriction. The Data Subject has the right to request that SMERU delete or restrict (i.e. SMERU may only store the data without further Processing) the Personal Data relating to the Data Subject or refrain from sharing such data with third parties in case the data is clearly excessive, no longer necessary in relation to the purposes for which it was collected or the Data Subject withdraws Consent, if Consent is the basis for Processing in accordance with paragraph 4.2.

7.4 Right to Object. The Data Subject has the right to object to the Processing of Personal Data relating to the Data Subject, unless SMERU can establish that there is a legitimate ground for the Processing in accordance with paragraph 4.2 and 4.3.

7.5 Right to Data Portability. The Data Subject has the right to request that their Personal Data be transmitted to the Data Subject or others designated by the Data Subject, in a structured, commonly used and machine-readable format, where technically feasible.

7.6 Right against automated individual decision-making including profiling. The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

7.7 The rights of the data subject mentioned in point 7.1 to 7.6 above can be waived for research purposes, matters related to law enforcement or other measures as regulated under Indonesia's laws and regulations.

7.7 A Data Subject may contact SMERU regarding any requests in relation to the exercise of these rights under this Section 7 through the dedicated email address dataprotection@smeru.or.id, indicating that the request concerns personal data. Such request will be forwarded to the IT Head of Unit (cc. the Institute Secretary) . The identity of the requester must be verified before complying with the request. The IT Head of Unit should provide a response within one month of the receipt of such request, which can be extended by another month depending on the complexity of the request. The response shall be in writing and explain the action to be taken or provide reasons if the request cannot be met. Letter for responses will be developed as needed.

7.8 The Data Subject whose request was not acted upon by SMERU has the right to raise a request for review of alleged violation of his or her rights under this Section 7 in accordance with SMERU's Compliance Review Mechanism (see Annex 3).

8. Storage

8.1 Personal Data shall be kept only as long as it is necessary for the relevant purposes or for the periods SMERU has notified to Data Subjects under Section 6. After these periods, the personal data shall be either deleted or kept in a form which does not permit identification of Data Subjects.

8.2 SMERU shall take appropriate technical and organizational measures to ensure a level of security appropriate to the risks and nature of the Personal Data to be Processed and to ensure protection against accidental or unlawful destruction or accidental loss, and to prevent unlawful forms of Processing, in particular unauthorized disclosure, dissemination or access or alteration of Personal Data.

9. Privacy by Design and Privacy by Default

9.1 SMERU will implement appropriate technical and organizational measures which are designed to implement the Policy, both at the time of the determination of the means for Processing and at the time of the Processing.

9.2 In particular, while designing a database and drafting procedures for collecting Personal Data, the principles of Processing of Personal Data and the rights of Data Subjects stipulated in this Policy must be taken into account and reflected accordingly.

9.3 SMERU will also implement appropriate technical and organizational measures for

ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are actually Processed.

10. Data Protection Impact Assessment

10.1 Where the Processing of Personal Data is likely to present high risks for the rights or freedoms of Data Subjects e.g. due to the type or amount of data or the number of Data Subjects or the purposes of the Processing, SMERU shall, in advance of the Processing, carry out a data protection impact assessment (DPIA) and address any issues such assessment may reveal. Examples of high-risk Processing include:

(i) systematic and extensive Processing activities (including profiling) where decisions have legal effects or similarly significant effects on Data Subjects; or
(ii) large scale Processing of Sensitive Personal Data.

10.2 A DPIA should include:

(i) a description of the envisaged Processing and the purposes of the Processing;
(ii) an assessment of the need for and proportionality of the Processing and the risks to Data Subjects arising; and
(iii) measures envisaged to mitigate those risks and ensure compliance with this Policy.
(iv) Members of a team will be specifically established to conduct the assessment when needed.

10.3 If an assessment indicates that the Processing may indicate a high risk, the Director must be consulted.

11. Data Breach Management Procedure

11.1 SMERU personnel are required to inform IT Head of Unit as soon as possible upon becoming aware of an actual or suspected Data Breach. IT Head of Unit immediately address the possible Data Breach by stopping all access to the Data, and immediately report the Data Breach to the Board of Directors.

11.2 SMERU will take the following measures to address an actual or suspected Data Breach:

a) Assessment consisting of:
   (i) data records and type of Personal Data affected;
   (ii) date, time, duration and location;
   (iii) cause of the Data Breach;
   (iv) list of affected Data Subjects;
   (v) risk of serious harm to Data Subjects; and
   (vi) risk of other adverse consequences (operational, security, financial, reputational); and
b) Measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the Data Breach.

11.3. Director may appoint a Data Breach response team who will carry out the assessment as described above, in cases involve a Data Breach is likely to result in a

high risk to the rights and freedoms of Data Subject. Such team include members from IT, HR and general affairs, business development, research personnel, and external experts as appropriate. The response team will submit a report to Director which includes the results of the assessment and recommendation on the measures to be taken in response to the Data Breach.

11.4. If a Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, under the Guidance of Institute Secretary as the Lead data Breach response team, IT Head of Department/ Research Head of Department/ other relevant Department which directly involve with Collection and Procession of Data Subject shall inform the Data Subject on the results of the assessments and take appropriate measures without undue delay. In such case, the Director shall be also informed.

12. Data Transfer

12.1 External data transfer: SMERU will ensure that Personal Data is only transferred under Section 5 to jurisdictions or international organizations that ensure adequate level of protection. Should it be necessary to transfer Personal Data to a third party that does not provide adequate level of protection, SMERU will ensure that it maintains appropriate safeguards such as entering into appropriate contractual clauses in order to safeguard Personal Data.

12.2 Internal Data Transfer: Data transfer within SMERU carried out between different components of SMERU are permitted to the extent that the data transfers are in accordance with this Policy and that all staff, interns, volunteers, secondees, individual consultants, and individual contractors involved in the internal data transfers strictly comply with the Policy. Strict adherence to this Policy is included in the obligations of staff under the SMERU existing regulations. Contracts with interns, volunteers, secondees, consultants, and contractors shall specifically include provisions requiring compliance with the Policy. Violations of the Policy will result in appropriate disciplinary measures for staff, while those involving contractors, consultants, interns, secondees, and volunteers will result in appropriate action under the terms and conditions of their respective contracts.

13. Implementation

13.1 The Policy may be complemented by guidelines as appropriate to provide further guide on the implementation of the Policy.

13.2 The Institute Secretary shall act as the data protection contact and is responsible for overseeing the application and implementation of the Policy throughout the organization under the the IT Head of Unit, Vice Director of Research, and Vice Director of Administration and Finance.

13.3 A committee comprising of Director, Institute Secretary, Vice Director of Research and Vice Director of Administration and Finance shall convene at least once a year to discuss and assess the needs regarding data protection issues. The meeting will include discussion on the monitoring of data protection practice with IT head of Unit and relevant personnel form

other departments/ units.

13.4 Regular review should be conducted at least every three years with a focus on data protection and security measures to monitor, assess and improve data protection practices/documentation. The director shall form a special team consisted of relevant unit to conduct comprehensive review to ensure that the policy will be updated in accordance to the latest regulations and best practices.

APPENDICES

Appendix 1: Categories of Protected Data & Procedures of data protection

1A. Categories of protected data

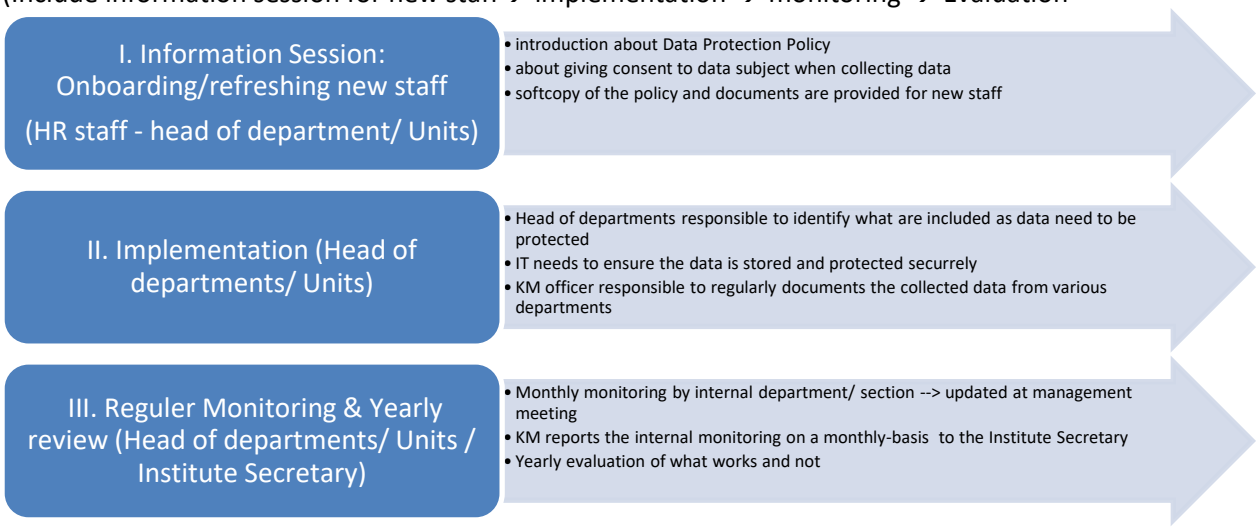
Department/ Sections	Categories of protected data	Mechanism to protect data (who have access/ how to secure sensitive information)
ALL DEPT	Data received from third parties	Based on Non-Disclosure Agreement/ Confidentiality Agreement/ Gentlemen agreement
Research Dept	Respondent data	Research team Head of Research Department Head of research and Outreach Division
	Enumerator and Local/Regional Researcher data	Human Resource Unit Team Leader Head of Research Department
	confidential data/ data under embargo	Research Team Head of Research Department Head of research and Outreach Division
	Other stakeholders' data	Communication Unit Knowledge Management Unit Business Development Unit
Publication	Data of respondents and specific locations (name of respondents, name of locations from the subdistrict down to the village level)	Confidential or sensitive data and information have been obscured or excluded in all documents submitted to the publications team. Data of respondents and specific locations (name of respondents, name of locations from the subdistrict down to the village level) are undisclosed in all studies published by SMERU or other organizations and are referred to under a false name. In some contexts, other information concerning the identity of the respondents, such as profession, age, and gender may be subject to concealment.
Business Development Unit	SLC user data	SLC raw user data can only be accessed directly by the IT team. The Management Team and busdev can ask the IT unit team to display the required data. SLC user data cannot be shown by other parties or units (SMERU internal) except with the approval of the Management Team and/or busdev. SLC user data may not be published to the public unless approval is obtained from the user concerned (for the purposes of testimonials or other marketing activities)
	Marketing dashboard data (Project details & budget)	The IT team can display SMERU's internal data (related to projects & finance) to busdev, to create a marketing dashboard, with the approval

		of the Director. Research & outreach and Dir. Adm. & Finance.. The marketing dashboard that displays the names of other institutions can only be accessed by the management team. The marketing dashboard can be displayed for all SMERU internal parties if it does not display the names of other institutions.
	Marketing Survey Data	Survey results data can only be accessed by the IT Team and busdev. The Management Team can ask the IT team and busdev unit to display the required data. External survey data may not be made public.
	Market research data (data sekunder)	Secondary data from various external sources and has been officially published is used by busdev for analysis and formulation of institutional strategic plans and can be accessed by all SMERU internal parties
HR	Staff's personal data (KTP, NPWP, CV, ijazah, dll)	Accessible by: HR, Kadep General Affairs, Finance & Kadiv Keu & Admin, IT, program admin Storage: HRIS, folder P HR Secured by: access level to HRIS, limited access to P folder as set by IT How others can request data? Need to fill in request form and approved & acknowledged by Kadep General Affairs
	Contract	Accessible by: HR, Kadep General Affairs, Finance & Kadiv Keu & Admin, IT Storage: HRIS, folder P HR Secured by: access level to HRIS, limited access to P folder as set by IT
	Evaluation of Individual performance	Accessible by: Kadiv Keu & Admin, IT Storage: HRIS & google link Secured by: access level to HRIS, user ID & password to access the link Raw data & analysis are presented to Directors. Upon approval of Directors, analysis can be distributed to individuals
	Data from management evaluation	Accessible by: Kadiv Keu & Admin, IT

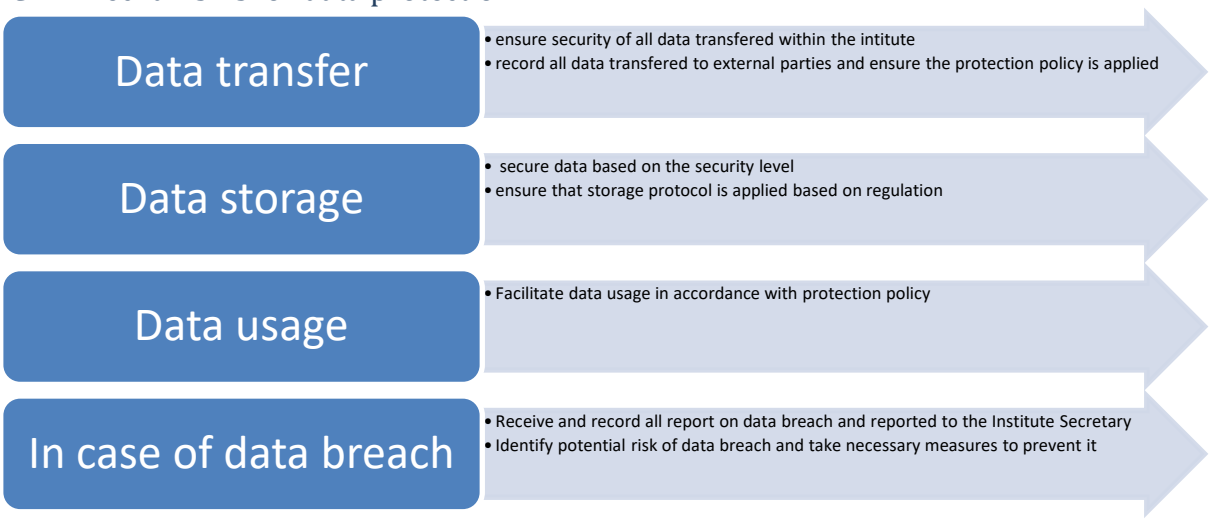
		Storage: google link Secured by: user ID & password to access the link Raw data & analysis are presented to Directors. Upon approval of Directors, analysis are presented to all staff
Keuangan	Staff's financial record (remuneration, allowance, loans, dll)	Accessible by: HR, Kadep General Affairs, Finance & Kadiv Keu & Admin, IT Storage: HRIS, Accounting and/or Finance (hard copy files) Secured by: access level to HRIS, password to softwares
Program Admin	Projects data (description, value, etc.)	Accessible by: all Storage: available in the intranet Only for internal usage
	Administrative data of resource person, consultant, etc. (ktp, npwp, cv, buku rekening, materi narsum, dll)	Accessible by: PA, Kadiv Keu & Admin, IT Storage: folder P with limited access Secured by: password to folder
	Foundation's legal document (akta, ijin kumham, sertifikasi merek, TDY, Ijin Yayasan, dll)	Accessible by: foundation administration and institute secretary Storage: folder P with limited access

1B. Procedures of data protection

(Include information session for new staff→ implementation → monitoring → Evaluation

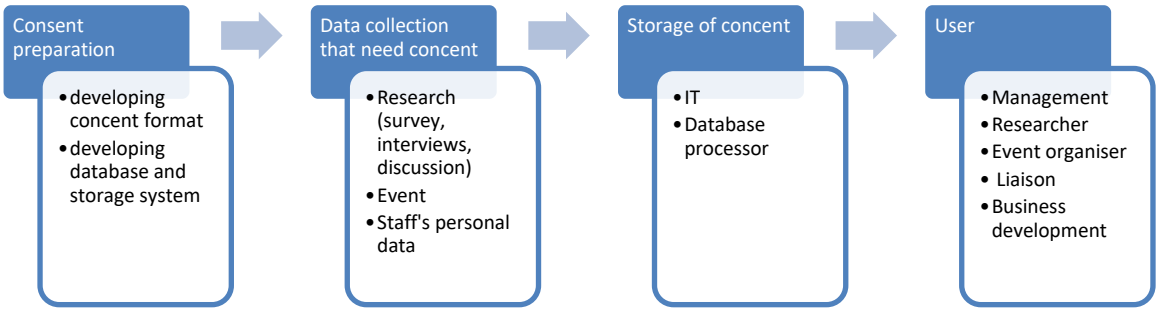


1C. IT mechanisms for data protection



Appendix 2: the Data Subject's Consent to the Processing of Personal Data

2A. Consent procedures

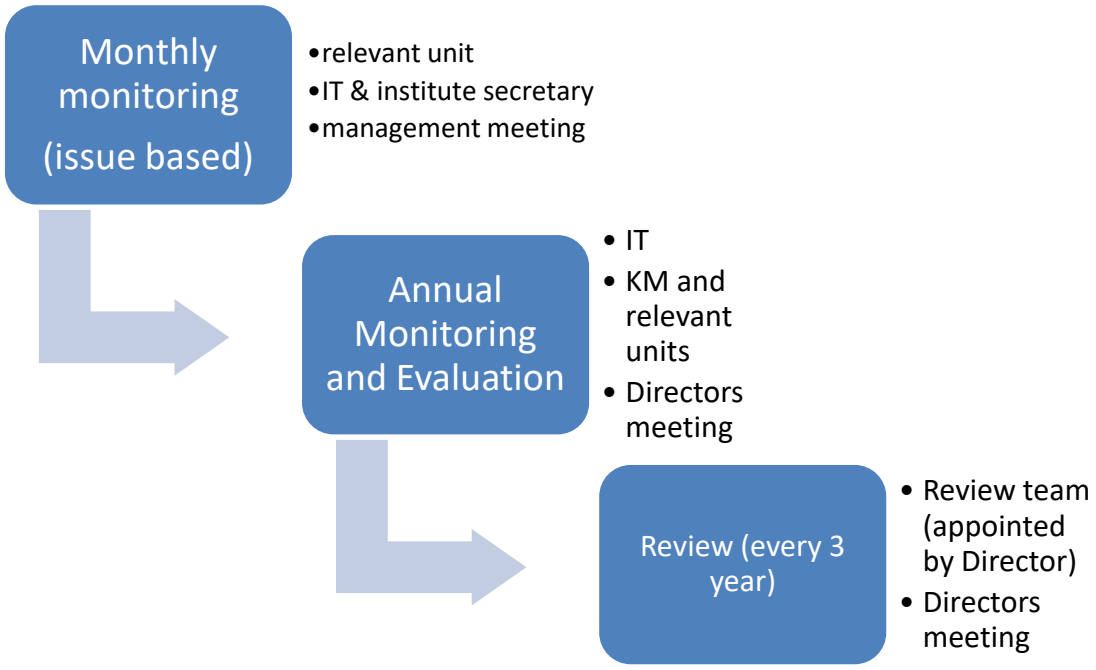


2B. Consent to the processing of Sensitive Personal data

SMERU ensures each responsible department/unit has procedures about providing information to the Data Subject either orally, electronically, or by filling in hardcopy templates.

At the time the sensitive Personal Data is obtained, SMERU shall provide the Data Subject the following information:
a) SMERU's contact details;
b) The type of Personal Data related to the Data Subject Processed by SMERU;
c) The purposes of the Processing;
d) Legal basis for the Processing;
e) The recipient or categories of recipients (third parties) that the Personal Data are to be disclosed to;
f) The period for which the Personal Data will be stored; and
g) How to exercise the Data Subject's rights set out in Section 7.

Appendix 3: Procedures for review



The SMERU Research Institute

Phone : +62 21 3193 6336

Fax : +62 21 3193 0850

E-mail : smeru@smeru.or.id

Website : www. smeru. or.id