

Data Protection Guidelines

March 2025

Table of Contents

I. PURPOSES AND SCOPE	1
II. DEFINITIONS.....	2
III. DATA PROTECTION PRINCIPLES AND MEASURES	4
1. The necessity requirement.....	4
2. Compliance with data protection principles	4
3. Processing sensitive data	7
4. Data protection impact assessment	7
5. The rights of the data subject.....	8
6. Managing data subject requests	11
IV. LIMITATIONS.....	11
V. DATA PROTECTION BY DESIGN AND DEFAULT.....	12
VI. RELATIONSHIPS WITH THIRD PARTIES.....	12
1. Data sharing	12
2. Outsourced data processing	12
3. Data transfers	13
VII. ORGANISATIONAL MEASURES.....	14
1. Data Mapping	14
2. Incidence management.....	14
3. Training	15
4. Record of data processing activities.....	15
5. Monitoring.....	15
6. Responsibilities.....	15
7. Internal Data Protection Policy.....	15
VIII. CONCLUSION: GENERAL INFORMATION SECURITY	16

I. PURPOSES AND SCOPE

1. Considering that data protection is a fundamental Human Right recognised by both the UN's Universal Declaration of Human Rights and regional Human Right charters, these Guidelines aim to:
 - a. promote data protection best practices in an international environment that is characterized by a rapid adoption of data protection rules and regulations by states and organizations;
 - b. meet the expectations of GIZ's commissioning parties, who require that assignments carried out by GIZ on their behalf comply with the highest standards, including those of data protection;
 - c. uphold the trust of the numerous data subjects involved in GIZ projects, who legitimately expect protection from GIZ and its partners with regard to their personal data;
 - d. protect Human Rights, since beside being a fundamental Human Right, failure to protect personal data could seriously affect other fundamental Human Rights of the individual, such as the right to life, integrity, security and liberty, non-discrimination, private and family life, and property; and
 - e. build trust and reputation and promote a cordial relationship between GIZ and its partners and contractors, for cooperation beyond the scope of a single project.
2. The Guidelines have been carefully designed to help GIZ's partners and contractors to meet an adequate level of data protection standards. Without creating any obligations for GIZ's political partners, the Guidelines are an orientation for fulfilling the data protection requirements contractually agreed between GIZ and a given contractor acting as an independent data controller, except where:
 - a. the contractor is subject to the GDPR; or
 - b. the Guidelines conflict with other legal obligations to which the contractor is subject.
3. Nothing prevents other categories of controllers from voluntarily using these Guidelines to better understand their respective data protection obligations.

II. DEFINITIONS

For the purpose of these Guidelines:

- 1) “**personal data**” means any information that alone or in combination with other pieces of information, can lead to the identification of an individual or be attributed to that person. It ranges from direct identifiers such as names, email addresses etc., to indirect or remote identifiers, such as IP address or just the exact time of one’s visit to a website. For an indirect identifier to amount to personal data, it is not necessary for all the additional information essential for the identification to be in the hands of the data controller or processor. Several remote identifiers in the hands of different controllers or processors would each amount to personal data if a combination of all the remote identifiers would lead to the person’s identification, except where obtaining this additional information from other controllers or processors is prohibited by law or involves disproportionate efforts (especially relating to time and high costs).
- 2) “**anonymous data**” means data that may contain some general information relating to natural persons but cannot lead to the identification of specific individuals or be attributed to them. It could be achieved by using among other things larger geographical groupings (naming cities, districts or regions, instead of associating the unidentified individuals with a village or smaller communities); generalizations and ranges (for instance, age range instead of one’s age or date of birth; salary range, instead of one’s exact salary); and statistics etc., to prevent the identification of individuals. Anonymized data is not personal data and as such, is not subject to the protection recommended by these Guidelines. However, depending on their relevance, they could be subject to information security requirements. (*See: Information security at the end of this document*)
- 3) “**processing**” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The simple act of receiving or sharing or granting access to personal data amounts to data processing, irrespective of whether additional operations are conducted on the data or not.
- 4) “**sensitive data**” means any personal data revealing one’s ethnic origin, or political opinions, religious or philosophical beliefs, or trade union membership, or genetic or biometric data, or data concerning health or data concerning a natural person’s sex life or sexual orientation. Other types of personal data, such as those relating criminal records, financial and location data, could also be considered sensitive, due to the degree of harm that their processing may cause to the rights and freedoms of the data subject (such as discrimination, stigmatization, or loss of assets, and in the case of location data, a threat to one’s life and security).

- 5) **“controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and the essential means of processing personal data. The purposes here refer to the “whys” of the processing, and the essential means involves decisions on whose and which data is to be processed, for how long should the data be processed, and who should have access to it. Decisions on non-essential means, such as a given hard- or software, could be delegated to the processor (a service provider, for instance) without making it a controller or a joint controller. However, any processor that goes beyond the instructions of the controller by determining additional purposes or essential means should be responsible for this additional processing, as a controller.
- 6) **“processor”** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. A processor is a third party and cannot be the controller’s employee. Contractors implementing projects associated with detailed data processing instructions from the commissioner are usually processors, just like website hosting and maintenance service providers.
- 7) **“consent”** means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For consent to be unambiguous, it must involve a clear affirmative action e.g. ticking a checkbox (but not opting out a pre-ticked checkbox). Silence would not qualify as acceptance. For sensitive data, the consent should be explicit. That is, affirmative action must be stronger. This is in general achieved through a duly signed document, a return email, an authentication (e.g. by SMS) or an electronic signature, to dismiss any doubts as to whether consent was given or not. Where the data subject is a minor or is incapable of granting consent due to some health or legal limitations, then parental consent or that of his or her guardian should be obtained. The controller should be capable of demonstrating that consent was actually granted.
- 8) **“data breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. It affects either the confidentiality, integrity, or availability of the data. In data protection, the concept of harm caused by such breaches is broadly construed. It must not necessarily involve reputational damage or financial losses. A mere loss of control over personal data or other form of distress would suffice.
- 9) **“data subject”** means an individual whose personal data is being processed. A data subject is a living natural person. That is, deceased persons are not covered by this definition, and thus their personal data is not protected by these Guidelines. Also, companies and other legal persons are not considered as data subjects, and as such their data is not protected by these Guidelines, except when the company’s or legal person’s information is that of an individual, like in the case of sole proprietorships.

- 10) **“encryption”** means a mathematical process used to scramble data or a message in order to make it unreadable except for the holder(s) of the keys. The recipient can decode or ‘decrypt’ the message using a specific key or password.
- 11) **“GDPR”** means the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- 12) **“profiling”** means any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- 13) **“pseudonymisation”** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures that prevent the identification of the data subject. Pseudonymized data is still personal data, although of a lesser quality, and a data breach affecting only pseudonymized data would be unharmed to the data subjects, since those having unlawful access to it would not have access to the additional information needed to identify the data subject. It is therefore a form of qualitative data minimization involving the assignment of pseudonyms such as special codes, numbers, or symbols to the data subjects, and safely hiding their personal data.

III. DATA PROTECTION PRINCIPLES AND MEASURES

In the absence of applicable stricter data protection legislation, the following requirements would help to comply with international data protection standards.

1. The necessity requirement

The very first point to consider before processing (collecting, using, receiving, sharing etc.) personal data is, whether the data is necessary for the attainment of the intended goal. Where the objective could be reasonably achieved with anonymous data (*as defined above*), then the processing of personal data would be unnecessary, and should not take place.

2. Compliance with data protection principles

Once it has been established that the processing of personal data is necessary, the following international standard principles should be complied with.

- a) **Lawfulness:** According to the protective purpose of informal self-determination, the processing of personal data should only take place if it is justified. This is always the case if:
- i. the data subject has been informed and has freely and unambiguously consented; or
 - ii. there exists an applicable legal basis for the processing. Examples of possible legal bases include situations where the processing is necessary for:
 - complying with a legal obligation to which the controller is subject;
 - the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - the performance of a task carried out in the public interest or in the legitimate interest of the controller, which must be balanced against the rights and freedoms of the data subject;
 - the protection of vital interests of the data subject or a third party; or
 - the establishment and defense of legal claims;
- b) **Purpose limitation:** Personal data should only be processed for specified, explicit and legitimate purposes defined by the controller or by the law. The processing should end, and personal data deleted upon achievement of the initial purpose, unless where a new purpose is compatible with the initial one. The following new purposes are judged compatible:
- i. where the new processing is required by the law;
 - ii. further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards (such as data minimization and pseudonymisation);
 - iii. processing aiming at exercising legal claims and defense; and
 - iv. where the processing involves the complete anonymization of personal data.
- Where none of these compatible grounds are applicable, the consent of the data subject should be obtained for the new processing operation.
- c) **Data Minimization:** Personal data should be quantitatively and qualitatively limited to only what is strictly necessary to achieve the intended purpose. Minimization should consider aspects such as limiting the number of data subjects involved (sampling); limiting the amount of personal data collected per

person; using less intrusive means or avoiding means that may uniquely identify the data subject (for example, preferring signatures to fingerprints; stating one's age instead his date of birth; taking pictures from a distance, to avoid bringing ordinary participants to the limelight etc.).

- d) **Accuracy:** Personal data should be accurate and, where necessary, updated; steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified immediately.
- e) **Storage limitation:** No personal data should be permanently stored. It should be stored in a manner that permits the identification of data subjects for a period not longer than necessary for the desired purposes. It should be immediately deleted, unless one of the exceptions mentioned in 2.b. (*purpose limitation*) applies. The deletion should be automatic and scheduled for given intervals.
- f) **Fairness and Transparency:** Fairness requires that the processing should not be unjustly detrimental to the data subject or go beyond the data subject's expectations. Also, the information provided to the data subject should not be misleading. Transparency requires the provision of sufficient information to the data subject, including information on who is processing which data, why, on what legal basis, where, how and for how long, who has access to the data, as well as any possible risks. The rights of the data subject (see 3.a-j) should equally be communicated to him or her.

However, the provision of information would not be necessary, if:

- i. the data subject already has such information;
- ii. the processing is expressly required by national law, which defines how the processing shall be carried out;
- iii. the information is subject to professional secrecy; or
- iv. the provision would involve disproportionate efforts, especially when a very large number of data subjects are involved. In that case, informing the general public through a radio or TV announcement would be appropriate.

Any information provided should be in simple and plain language, in a way that any ordinary person can understand. Where appropriate, symbols could be used.

- g) **Integrity and Confidentiality:** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage of personal data. Typical technical and

organizational measures such as but not limited to the pseudonymization and encryption of personal data, should:

- i. ensure the ongoing confidentiality, integrity, availability of personal data and resilience of processing systems and services;
 - ii. restore the availability and access to personal data (back-up) in a timely manner in the event of a physical or technical incident; and
 - iii. put in place a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- Persons acting under the controller's authority should process personal data only with the controller's documented instructions. Only those whose roles are directly related to the processing of personal data should have access to the data, and they should conclude confidentiality agreements. The engagement of third parties such as service providers, should equally be regulated (*see... under Organizational measures*).
 - Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements of this provision.
- h) **Accountability:** The controller should implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with these Guidelines and other data protection obligations to which it is subject. Such measures should be reviewed and updated where necessary, and may include the recording of data processing activities and the adherence to a data protection code of conduct or an approved certification mechanism.

3. Processing sensitive data

Due to the high risks associated with the processing of sensitive data (*defined above*), their processing should be in principle be avoided, except where such processing is expressly authorized by the law to which the controller is subject, or where the data subject has given his explicit consent, or where the processing is necessary to protect the vital interests of the data subject or of another natural person if the data subject is physically or legally incapable of consenting.

4. Data protection impact assessment

Taking into account the nature and extent of the data processing, the sensitivity of the data, the category of data subjects involved as well as the technology employed, a operation could be associated with high risks.

- a) The controller should therefore conduct an impact assessment, to identify such risks and take measures to mitigate them, prior to commencing the processing. Processing operations associated with high risks include:
 - i. Evaluation or scoring, including profiling and predicting, especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements;
 - ii. Automated-decision making with legal or similar significant effect,
 - iii. Systematic monitoring, to observe, monitor or control data subjects, including data collected through networks or a systematic monitoring of a publicly accessible area;
 - iv. The processing of sensitive data or data of a highly personal nature (*see...under definitions*);
 - v. Data processed on a large scale;
 - vi. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject;
 - vii. Innovative use or applying new technological or organizational solutions;
 - viii. when vulnerable data subjects such as children, patients and refugees are concerned; and
 - ix. When the processing in itself prevents data subjects from exercising a right or using a service or a contract.
- b) The impact assessment should consist of at least the following parts:
 - i. an extensive description of the processing operation (its goal, legal basis, expected duration, parties involved, tools used, processes, personal data and data subjects involved, data transfers);
 - ii. an evaluation of the proportionality of the processing (data minimization);
 - iii. an extensive examination of the possible risks (emanating from the tools and persons involved, or third parties such as hackers and those threatening the confidentiality, integrity and availability of the personal data);
 - iv. and mitigation measures to counter the risks.
- c) In evaluating the risks, the controller should adopt an *inclusive* and *do not harm* approach and may consider associating the data subjects involved by soliciting their opinions.
- d) The processing should only take place when the risks have been sufficiently mitigated, and the outcome of the assessment should be documented and integrated into the processing operation.

5. The rights of the data subject

The processing of personal data should take into account and facilitate the exercise of the following rights.

- a) **The right to fair and transparent information and communication:** This should be an obligation for the data controller to comply with, without waiting for a request from the data subject. When collecting personal data from the data subject or within a reasonable time if obtained from a third party, the controller should provide the data subject with all the necessary information relating to the data processing (see *details in paragraph 2.f. Fairness and transparency principle, including exceptions*). Where the personal data is collected from a third party, in addition to the *information in 2.f.*, the controller should state the source of information, and where several channels are used to collect personal data and it is difficult to identify a particular source, general information regarding such sources should be stated.
- b) **The right of access:** The data subject should be able to obtain from the data controller, a confirmation as to whether or not personal data concerning him or her are being processed and, if it is the case, to receive a copy of such data and detailed information about the processing operation, including information required by paragraphs *2.f. and 3.a.*
- c) **The right to rectification:** The data subject should be able to obtain from the controller without undue delay, the correction of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject should have the right to have incomplete personal data completed.
- d) **The right to withdraw consent:** The data subject should be able to revoke his or her consent at any time. Once this is requested, the controller should immediately stop processing the personal data. The withdrawal of consent would not affect the lawfulness of processing that occurred before the withdrawal. Hindering or preventing the revocation of consent would imply that such consent is not freely given, since “freely” means one can deny or withdraw consent without suffering any detriment. Revoking consent should therefore be as easy as the manner in which the consent was initially granted.
- e) **The right to erasure:** In addition to the storage limitation principle mentioned above, the data subject should be able to obtain from the controller, the erasure of personal data concerning him or her, and the controller should proceed with the erasure, if:
 - i. (i) the data subject’s consent has been withdrawn and there is no other legal basis;
 - ii. (ii) the personal data is no longer necessary for the intended purpose;
 - iii. (iii) the personal data was processed unlawfully, or the erasure is required by law.

However, even with a pending request for erasure, the controller may continue with the data processing if the further processing is compatible (*see: ...purpose limitation*).

- f) **The right to object to processing:** Whenever the processing of personal data is based on public interests or the legitimate interests of the controller instead of the data subject's consent, the data subject should be able to object to such processing at any time. Once this right has been exercised, the data processing must stop and the personal data needs to be deleted, unless the controller can demonstrate that it has compelling legitimate interests in such processing, that override the data subject's rights and freedoms. However, such interests cannot be said to be compelling when the processing is carried out for marketing purposes.
- g) **The right to restriction of processing:** The data subject should be able to restrict the processing of their personal data under certain circumstances, for instance, where the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data. In the case of digital platform, it should be possible for the data subject to restrict the processing of his account data by deactivating it himself, instead of deletion.

Whenever this right is exercised by the data subject, any other form of processing should be stopped and profiles deactivated (but not deleted), and the personal data should be safely stored and access to it significantly restricted, while permitting a future continuation of processing, including the reinstatement of deactivated profiles, except where erasure becomes the outcome.

- h) **The right not to be subject to automated decision-making:** The data subject should not 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. The controller should take this right into account without any prior action from the data subject.

For example, no digital tool should be employed to take decisions in areas such as the cancellation of a contract; entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit; or admission to a country or denial of citizenship. Other types of automated processing that may seriously affect the data subject include those having significant effect on the circumstances, behavior or choices of the individuals concerned or having an impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals. Processing relating to access to credit or financial rewards, university admissions or admission to training programs, job applications are concrete examples.

However, automated decision making may still take place with the data subject's explicit consent and subject to a reasonable human intervention from someone capable of influencing the decision. Also, local law may permit such processing. It may as well take place if it is necessary for entering into, or performance of, a contract between the data subject and a data controller.

- i) **The right to data portability:** Where personal data is processed by automated means and based on consent, the data subject should have the possibility to

receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format. The data subject should equally have the possibility to transmit the personal data to another controller without hindrance from the controller to whom the personal data has been provided.

- j) **The right to complain with the competent authority:** If a local data protection supervisory authority exists, the data subject should have the possibility to lodge a complaint with it. The address of the supervisory authority should be communicated to the data subject.

6. Managing data subject requests

The controller should facilitate the exercise of data subject rights under Paragraph 5.b) to j). Where the controller is not in a position to identify the data subject, the controller should inform the data subject accordingly, and if possible, obtain additional information. The controller should not refuse to act on the request of the data subject, unless the controller demonstrates that it is not in a position to identify the data subject. Whenever a request is made;

- a) the controller should inform the data subject on action taken without undue delay, and in any event within one month of receipt of the request. In some cases there might be a need for an extension of two further months, taking into account the complexity and number of the requests. The controller should inform the data subject of any such extensions together with the reasons for the delay.
- b) if the controller does not take action on the request of the data subject, the controller should inform him or her without delay, of the reasons for not taking action, and where applicable, on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

IV. LIMITATIONS

The national law to which the controller is subject may provide some exceptions to the obligations and rights under Paragraph 4, requiring the restriction of the rights and freedoms of the data subjects. Such restrictions could occur especially in the following areas: national security; defense; public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; other important objectives of general public interest of its national law; the protection of judicial independence and judicial proceedings; the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority; the protection of the data subject or the rights and freedoms of others; and the enforcement of civil law claims.

Whenever the controller is relying on such exceptions, restricting the rights and freedoms of the data subjects provided here should strictly be in conformity with the law providing for such derogations, especially with regard to the purposes of the processing or categories of processing; the categories of personal data; the scope of the restrictions; the safeguards to prevent abuse or unlawful access or transfer. The data subjects should be informed about the restrictions, unless where providing such information would be prejudicial to the purposes of the restriction.

V. DATA PROTECTION BY DESIGN AND DEFAULT

Special attention should be paid to the embedding of technical features into data processing systems at the stage of their conception, to ensure and facilitate compliance with data protection principles and rights. This is the purpose of Annex 1 *“Data protection standards for developing digital tools meant for GIZ’s partners”*.

Measures should equally be put in place to ensure that an already existing system meets the requirements of Annex 1, before it can be used by the controller or anyone working under its authority. Even simple tools such as Excel sheets should be designed in accordance with the relevant data protection principles, especially that of data minimization.

VI. RELATIONSHIPS WITH THIRD PARTIES

1. Data sharing

Before disclosing personal data to independent third parties (parties other than processors) either by transmission or by granting access or otherwise, the controller should define and limit the use of such data, and impose some data protection obligations, either by way of contract with the recipient or through any other legally binding instrument. The contract should take into account the data protection requirements provided in these Guidelines, especially the principles and rights of the data subject. This position should not be considered if such sharing is expressly required by law to which the controller is subject.

2. Outsourced data processing

Where processing is to be carried out on behalf of a controller (including the provision of hosting or maintenance services), the controller should use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of these Guidelines. Factors such as expertise, experience, certifications and adherence to codes of conduct could be used in evaluating such processors.

Processing by a processor should be governed by a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the

type of personal data and categories of data subjects, and the obligations and rights of the controller. That contract or other legal act should stipulate, in particular, that the processor:

- a) shall not engage another processor without prior specific or general written authorization of the controller;
- b) processes the personal data only on documented instructions from the controller, unless required to do so by national law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- c) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- d) takes all measures required pursuant to the principle of integrity and confidentiality;
- e) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the applicable law requires storage of the personal data; and
- f) makes available to the controller all information necessary to demonstrate its compliance with the obligations laid down the contract and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

3. Data transfers

The controller should take measures to ensure that personal data does not receive lesser protection as a result of it being transferred to another country (by way disclosure or granting access). The transfer of personal data to a third party located in a different country with inadequate data protection standards should therefore be to be accompanied by certain measures. Such considerations may equally apply when the personal data is transferred to a third party that is physically present in the controller's home country, but not subject to its jurisdiction, especially when the third party is an embassy of a foreign country or an intergovernmental organization. Such measures include:

- a) identifying countries and organizations providing adequate data protection, where data transfers would not raise concerns ;
- b) conducting an impact assessment on the legal situation of countries identified as not providing adequate data protection, to see if any legal provision of such countries could hinder third parties therein from complying with their data protection contractual obligations; and
- c) contractually requiring stricter data protection measures, such as but not limited to encryption, pseudonymization and data minimization. Such measures should regulate all other aspects of data protection and cover onward transfers from the recipient to other third countries or international organizations.

The provision of an adequate level of protection by the third party's jurisdiction should not prevent the contractor from implementing measures pertaining to data sharing and outsourced data processing.

VII. **ORGANISATIONAL MEASURES**

To facilitate compliance with these guidelines, the controller should implement the following organisational measures.

1. Data Mapping

The controller should conduct an inventory of all the personal data it processes, identify the sources, categories, storage locations and duration of the processing. Such measures could facilitate location of personal data and take appropriate action, whenever data subjects exercise their rights.

2. Incidence management

The following measures should be adopted to manage data breaches.

a) Breach preparedness

In addition to the security measures required, the controller should define measures to be taken in case of a data protection breach and train those directly involved in implementing such measures. Also, those involved in the processing of personal data should be capable of identifying threats and know where to report them.

b) Breach notification

In case of a breach, the controller should notify the competent supervisory authority. The affected data subjects should equally be notified as soon as possible, if the breach poses a threat to their rights and freedoms, as pointed out in (*under definitions*). The information to be provided to the data subject should be detailed enough and should include: the nature of the breach; potential risks that he or she might be exposed to; measures adopted by the controller to mitigate the risks; recommended measures to be adopted by the data subject; and any other information that might be useful to the data subject, except where the applicable law provides otherwise.

Such notifications should take place without any unnecessary delay, suitably within 72 hours from the time the controller becomes aware of the breach, unless other notification period is determined by local law.

Neither the supervisory authority nor the data subject should be notified, if the technical and organizational measures implemented by the controller sufficiently mitigate the risks of such a breach. For example, if the personal data is encrypted or pseudonymized.

3. Training

The controller should periodically organize training sessions for its employees that have access to personal data. Such employees should be familiar with the provisions of these Guidelines that directly concern them.

4. Record of data processing activities

The controller should record each data processing operation. That record should contain the following information: the name and contact details of the respective unit of the controller and, where applicable, the joint controller, and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organizations; where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization; where possible, the envisaged time limits for erasure of the different categories of data; and where possible, a general description of the technical and organizational security measures.

5. Monitoring

The controller should adopt measures to periodically assess its degree of compliance with these guidelines, including internal evaluations and external audits. The legal environment should equally be monitored, to see if any law has been enacted that hinders the exact implementation of these guidelines or imposes additional obligations on the controller.

6. Responsibilities

To oversee compliance with these Guidelines, the controller should designate a data protection officer, who can be one of its employees having appropriate qualification and experience or an external natural or legal person active in the field of data protection. The duties of the data protection officer should be clearly defined, including: being the contact person for all data protection matters; advising the management on data protection; training employees; providing opinion on all data processing operations; and performing any other appropriate task. The data protection officer should be subject to confidentiality, either by contract or by law.

The controller should provide the data protection officer with means and resources to independently execute his duties, including further training on data protection and relevant certifications.

7. Internal Data Protection Policy

The controller should establish a data protection policy that transposes the provisions of these Guidelines into its internal rules and regulations. Also, it should establish templates of the necessary data protection documents, to facilitate future data processing operations. Such documents may include: a data protection policy; a

consent form; a data protection notice for its websites; a data protection impact assessment; an anonymous questionnaire; an outsourced data processing contract; and a data sharing agreement and a record of processing activities. These templates should be regularly reviewed and updated.

VIII. CONCLUSION: GENERAL INFORMATION SECURITY

Although these Guidelines aim at protecting personal data, applying its relevant provisions (especially *paragraphs...Integrity and confidentiality & data protection by design and by default*) to all other categories of valuable information could help achieve a reasonable standard of general information security.

Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, with a view of ensuring confidentiality, integrity, and availability. While there cannot be data protection without information security, the latter differs from the former in that it has a broader scope and protects other forms of information that might not necessarily amount to personal data. Information security might therefore cover everything, including trade secrets, internal documents, processes, and other forms of anonymous data.

For instance, a mere company's internal procedure (involving no personal data) should be subject to information security, since a third party might use such information to trick employees of that company into believing that he works there, and thus giving the third party the possibility to harm the company. Also, a survey report that shows that farmers from a given district have made huge financial gains would be considered sensitive information in a fragile context, even when the report is completely anonymous. This is because all the farmers from that district could be targeted.

So therefore, anonymous information and systems containing them should be subject to confidentiality, integrity, and availability, if their misuse would expose the controller or third parties (natural or legal persons) to harm.