Table of Contents

Concept Note on the Protection, Security, Processing, and Safeguarding of Personal Data of the National Commission for the Missing and Forcibly Disappeared in Lebanon

Explanatory Statement

Establishing frameworks to protect, safeguard, and process personal data, in addition to setting laws and procedures for this purpose, are a persistent and necessary need which allows the National Commission for the Missing and Forcibly Disappeared ("the Commission"), in charge of handling such data, to prevent incurring financial, legal, and procedural repercussions, as well as influencing the reputation and integrity of the Commission.

Law No. 105/2018 granted the Commission the mandate to collect and process personal data for humanitarian purpose, in order to identify the whereabout of missing persons.

Article /36/ of Law No. 105/2018 states that the Book of Regulations for the Management of the Central Records of the Missing and Forcibly Disappeared Persons, is subject to the approval of the Commission, which requires drafting the Book of Regulations for the Management of the Central Records of the Missing and Forcibly Disappeared Persons, including the protection, security, processing, and safeguarding of personal data of the Commission in Lebanon.

On the procedural level, most personal data protection laws give individuals rights related to their personal data, such as the right to access and remove their information. Moreover, non-compliance with personal data procedures may result in operational setbacks in the Commission, which requires the Commission to set substantial principles for the protection of personal data.

In this context, most laws relating to personal data protection are based on principles that represent the basis for everything relating to the privacy, protection, and processing of personal data. These principles create an adequate environment for institutions to abide by said principles when processing personal data in order to protect it. These principles are the following:

- Lawfulness, equity, and transparency principles when processing personal data.
- Determining a specific goal when processing data, i.e., accessing and processing the least amount of data for a specific legitimate goal.
- Limiting the amount of processed data in order to include the least amount of personal data.
- Ensuring accuracy and that the data is up to date, in addition to implementing needed procedures to correct and update inaccurate information.
- Limiting data retention period measures, given that personal data should not be retained for longer than necessary.
- Integrity and confidentiality, given that the Commission shall enforce security measures to prevent losing, damaging, or removing personal data.
- Accountability, given that mechanisms and schedules shall be set to prove compliance with applicable laws.

Processing Principles:

Personal data shall be:

- Processed according to Law 105, in an equal and transparent manner for the Data Subject.

- Collected for defined, expressed, and legitimate goals. Data shall not be processed in a way that contradicts the goals and principles of the Commission, or law 105. Processing for archiving purposes by the Commission, or for scientific or historical purposes, or for statistical purposes, is not considered as contradictory to the stated goals.
- Maintained as long as necessary for archiving purposes by the Commission, or for scientific or historical purposes, or for statistical purposes, provided that technical and organizational measures required by virtue of Law No. 105/2018 be taken in order to protect the Data Subjects' rights.
- Processed in a manner which guarantees data integrity, including protection from illegitimate or illegal processing, breach, loss, destruction, or damage by taking adequate technical and organizational measures.

The Commission shall, as to its role in dealing with personal data as a Data Controller, abide by certain conditions. The Commission is the authorized entity to decide on the purpose and the means for processing the data,

And it shall be liable in respect of complying with its responsibilities, including abiding by the following:

- Data protection principles.
- Users' rights.
- Data breach management.
- Respect of the principles set forth in Law 105.
- Dealing with authorized Data Processors and essential guarantees providers in order to protect data.

When dealing with personal data, it is essential to abide by the paramount principle whereby all personal data shall be processed in a legal and fair manner. In this sense, the Commission shall implement/fulfill at least one of the following conditions to process data:

- Obtain the consent of the individual/user to process their personal data.
- Legitimate/justified interest (need): it is crucial to have a justified need to involve third parties.
- Contractual necessity: necessary or conditional data processing in order to be able to enter into or conclude a contract.
- Legal obligations: the Commission is required by Law 105 to process personal data,
- Vital necessity/urgency: personal data processing is essential to maintain or protect the lives of individuals/users.
- Public interest according to Law 105
- Sensitive data is only processed upon the explicit consent of the individual/user, or in accordance with Article 2.2 In addition, sensitive data may be processed if this data is required to file a legal proceeding or claim as per Chapter 6 of Law 105 (punitive provisions).

In this context, the Commission shall follow the below-mentioned ten steps to implement the Personal Data Protection Program:

1- Appoint a Data Protection Officer: multiple data protection laws addressed the "Data Protection Officer" (DPO) principle. It is a position aiming to supervise the Data Protection Program of the Commission and ensure compliance with applicable laws. The job of the DPO may be assigned to an employee that is already available in the Commission or to a new employee. The DPO shall be independent, expert in data protection and safety, and proficient in this field, and submit reports to the highest management levels. The DPO shall help in supervising internal compliance with the applicable data protection laws and advise the Commission on its obligations to protect data, in addition to working as the focal point for individuals and data protection entities.
2- Maintain the Personal Data Record: in order to preserve personal data, the Commission shall be aware of the data it collects, how it is used, and how it is stored. This is achieved by identifying and documenting all processes within the Commission that involve personal data, how and why it is used, as well as where and for how long it is stored within the Personal Data Record. The Record shall include:
    - The name and contact details of the DPO and any third party.
    - The legitimate bases and goal of data processing.
    - The different types of processed data.
    - Personal data processing systems and locations.
    - Data transfer locations and list of Recipients.
    - Data storage period and required technical and security measures.
3- Send a notice regarding the goal from this Program and obtain approval; given that transparency is a cornerstone of personal data processing laws.
4- Respond to individuals' requests/inquiries on their personal data.
5- Implement and impose security mechanisms.
6- Ensure data privacy, procedures, and services in an embedded system.
7- Send a notice upon the occurrence of a data breach.
8- Manage third parties.
9- Protect personal data when transferring it
10- Publish the Commission data protection policies, procedures, and practices.

The Book of Regulations for the Management of the Central Records of the Missing and Forcibly Disappeared Persons, namely the Protection, Security, Processing, and Safeguarding of Data, including the Personal Data of the National Commission for the Missing and Forcibly Disappeared in Lebanon

These bylaws are a public document, made available on the website of the Commission.

Article 1: Definitions

Commission: The National Commission adopted and defined in Law No. 105/2018 (Law 105) as the only Commission in charge of implementing this Book of Regulations and all assignments.

Scope of Application:

1- Provisions stipulated herein shall be applied on all automated and manual personal data processing of the missing and forcibly disappeared in Lebanon by the Commission.
2- Provisions stipulated herein shall be applied when processing is conducted in Lebanon.

General Data and its Categories:

Data on the missing and forcibly disappeared, in addition to the remains, is exclusively limited, by Law No. 105/2018:

- Data: organized or unorganized collection of data on the missing or forcibly disappeared, or facts, concepts, instructions, observations, or measurements, in the form of numbers, letters, words, symbols, pictures, videos, signals, voices, maps, or any other form, which are interpreted, exchanged, or processed via individuals or computers, including information mentioned anywhere herein, subject to Article /4/ (Confidentiality) of the Commission bylaws.
- Personal Data: any data relating to the missing or forcibly disappeared, which allows the Data Subject identification, whether directly or indirectly, through establishing links between data, by using identification elements such as their name, voice, identification number, personal electronic identification, geographical location, one or more physical, physiological, economic, cultural, or social characteristics, including sensitive personal data and vital biometric data.
- Sensitive Personal Data: any data that relates whether directly or indirectly to the missing, forcibly disappeared, or Data Subject, or uncover, whether directly or indirectly, the family, ethnic origin, political or philosophical opinions, religious beliefs, personal criminal record, or personal vital biometric measurements data thereof, or any data relating to their health, including their physical, psychological, mental, genetic, or sexual health, or remains, including data on health and social care providers thereto which uncover their health situations, and mass graves.
- Biometric Data: personal data resulting from a specific technical processing relating to physical, physiological, or behavioral properties of a natural person, which enables the identification or confirmation of the unique identity of this natural person, such as face images, fingerprints, dactyloscopy data, or other data.

Data Subject: the natural person subject of the personal data.

Personal Data Protection Officer (or DPO): within the Commission, the person who informs, advises or addresses recommendations to the data Commission. The DPO advises on whether or not to carry out a data protection impact assessment. the DPO collects information to identify processing activities. S/he analyses and verifies compliance of processing activities with the applicable law. The DPO is not in charge of the compliance, which is the responsibility of the Commission.

Personal Data Recipient: person authorized to receive personal data, distinct from the personal Data Subject, DPO, or the Commission.

Controller: the Commission is the controller of the personal data. In addition, other organisations may be co-controllers of the data.

Processor: a natural person or an entity that processes personal data on behalf of the Commission or under the Commission's directions and instructions.

Processing: any operation or group of operations, whether automated or not, carried out on personal data, including, *inter alia*, collection, record, organization, structure, storage, adaptation, change, retrieval, consultation, use, transfer (whether electronically, orally, or in writing), publishing, provision, correction, or destruction. "Operation" and "Processing" shall have connected meanings.

ID Masking Mechanism: through the processing of personal data in a manner to conceal the Data Subject's identity, not connect nor attribute this data to the Data Subject and avoid identifying them in any way whatsoever.

Automated Processing: processing carried out by using an electronic program or system which works in an automated and *impromptu* manner, whether totally independent, not requiring any human intervention, or partially independent, requiring a limited human intervention and supervision.

Personal Data Security: a group of specific technical and organizational measures, procedures, and operations, as defined herein, which maintain privacy, confidentiality, safety, integrity, coherence and availability of personal data.

Data Masking Mechanism: personal data processing in a manner which leads, upon processing completion, to the inability to link or assign such data to the Data Subject without resorting to additional information, under the condition that such additional information be independently and securely preserved, according to specific technical and organizational measures and procedures by virtue of the present Book, in order to ensure that personal data not be connected to a specific natural person or a natural person who can be identified through such data.

Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized disclosure of, or access to – Personal Data transmitted, stored or otherwise processed.

Profiling: an automated processing method where personal data is used to assess specific personal aspects relating to the Data Subject, including analyzing or predicting aspects relating to the Data

Subject's performance, financial situation, health, personal preferences, interests, behavior, location, movements, or credibility.

Cross-Border Data Processing: publishing, using, displaying, sending, receiving, retrieving, employing, sharing, or processing personal data outside the geographic scope of the State.

Consent: means any freely given, specific and informed indication of his or her wishes by which a Data Subject signals agreement to the Processing of Personal Data relating to him or her.

In case the processing is based on the consent of the Personal Data Subject, the following conditions must be met:

- The Commission must be able to prove that they have obtained the consent of the Data Subject for processing.
- The Personal Data Subject should be informed that they can withdraw their consent at any time, without affecting the legality of the processing carried out before the date of withdrawal, which remains subject to the provisions of this document. In particular, the data subject must be informed of the situations where the Commission may bypass their refusal (ex: for the transfer of their data to their parties as per Article 2.2, or the exceptions to their right to Correct or Remove Personal Data as per article 11; the exceptions to their right to Restrict Processing as per Article 12; the exception to their right to object to the Processing and Automated Processing of their data as per Article 14), and an information notice must be provided accordingly.

Article 2: legal bases for processing the data

2.1. Principle

The Commission is mandated to work for purely humanitarian purposes, namely to clarify the fate and whereabouts of the Missing and Forcibly Disappeared, pursuant to Law 105. The Commission's work encompasses the missing and forcibly disappeared. Thus, this enables the Commission to work on controlling and processing data under the following conditions, and as such, the legal bases for the Commission to process personal data under Law 105 include:

- Processing shall be necessary to protect the public interest, that is necessary to clarify the fate of the missing and forcibly disappeared.
- Processing shall be necessary for the purpose of archiving, or for scientific, historical, or statistical studies according to the Commission laws and regulations.
- Processing shall be necessary for the performance of the Commission's obligations as determined in Law 105.
- The Commission has obtained and recorded the consent of the Data Subject.

2.2. Specific situation of transferring the data to a third party including a foreign country or international organization

2.2.1. Personal data transfer to a third party is only allowed when the Commission considers, by virtue of the decisions it has issued, that these parties guarantee a sufficient level of protection of this data, by virtue of the rules and regulations applicable to the Personal Data Recipient.

2.2.2. In principle, the Commission must obtain and record the consent of the Data Subject before transferring any of their data to a third party and the purpose of the transfer must be purely humanitarian.

2.2.3 By exception, when it is impossible to contact the person or when the latter does not consent to the transfer of their data, and only when the purpose of the transfer is to clarify the fate and the whereabouts of the missing persons according to Law 105, the Commission may still transfer the personal data if all of the following conditions are met:

1. The Commission shall review the situation in order to assess the reasons for the refusal of the data subject, and
2. The Commission has run a risk assessment to ensure that the transfer may not create risk for the Data Subject, and
3. The Commission has signed an agreement with the third party in order to clarify the conditions under which this third party may use the data transfer, and the security of the data once transferred
4. The sole purpose for the Commission to transfer the personal data may be to clarify the fate and whereabouts of the missing persons, and
5. The Commission has informed the Data Subject that it will transfer their data despite their refusal, and before such transfer is done.

Article 3: General Obligations of the Commission

The Commission shall abide by the following:

- Take adequate technical and organizational procedures and measures in order to apply the appropriate benchmarks to protect and ensure personal data in order to maintain their confidentiality and privacy and to guarantee personal data not being breached, destroyed, changed, or tampered with, without prejudice to the nature, scope, and purposes of the processing, as well as the possible risks on the confidentiality and privacy of the Data Subject's personal data.
- Enforce adequate measures, whether when determining processing methods or during the processing operation itself, and such in order to comply with the present Book and the regulations stipulated in "Data Masking Mechanism Measures".
- Enforce adequate technical and organizational measures relating to automated settings in order to ensure that personal data processing is limited to the purpose set thereto. This obligation applies to the volume and type of collected personal data, and to the used processing type, in addition to the data storage period and the possibility to access it.
- Keep an electronic/specific record for personal data, provided that this data record contains all the Commission's and DPO's data, in addition to the description of the Commission's personal data categories; data of the persons authorized to access personal data; the processing period, restrictions, and scope; the Commission's mechanism to remove,

modify, or process personal data; the processing purpose; and any data relating to the cross-border movement and processing of such data, as well as the technical and organizational procedures especially relating to the security of information and processing operations,
- Any other obligations which may be determined based on the Commission work development and flow.

Article 4: The General Commitments of the service providers

When contracting service providers, the Commission shall ensure that it has sufficient guarantees to enforce technical and organizational measures as to guarantee that the processing operation meets processing requirements, rules, and regulations.

In particular, the Commission shall ensure that the service providers:

- Carry out and enforce the processing operation, in addition to the contracts and agreements concluded between them and the Commission, which particularly determine the processing scope, subject, purpose, and nature, the personal data type, and Data Subject's categories, as per the Commission's instructions.
- Apply the adequate technical and organizational measures to protect personal data in the design phase, whether when determining processing methods or during the processing operation itself, provided that the Provider takes into account these procedures and measures application costs, in addition to the nature, scope, and purposes of the processing.
- Carry out the processing operation according to the purpose and period determined thereto. In case the processing operation exceeds the period determined thereto, the Provider shall notify the Commission thereof in order for the Commission to allow the prolongation of the mentioned period or give them the appropriate directions.
- Remove data after the end of the processing period or after handing over the data to the Commission.
- Protect and ensure the processing operation, in addition to ensuring the electronic methods and equipment used in the processing and the personal data therein.
- Keep a special record for personal data which is processed on behalf of the Commission.
- Keep a record of the data of the people authorized to access personal data of the missing and their families; the processing period, restrictions, and scope; the Provider's mechanism to remove, modify, or process data; the processing purpose; and any data relating to the cross-border movement and processing of such data, as well as the technical and organizational procedures especially relating to the security of information and processing operations, provided that the Provider makes such report available to the Commission upon request.
- Provide all means to prove that the Provider abides by the present Book/Regulations upon the Commission request.
- Carry out and enforce the processing according to the rules, conditions, and regulations as determined in this Book and its implementing regulation, or by virtue of which the Commission's instructions are issued.
- Processing shall be enforced according to a written contract or agreement clearly determining obligations of Providers, duties, and roles in the processing operation.

Article 5: Reporting a Personal Data Breach

The Commission, with the support of the DPO, shall promptly address any personal data breach. The Commission shall issue a report that includes:

1- Statement on the nature of the breach or violation, the form and reasons thereof, as well as its approximate number and records.
2-
3- Potential and foreseen effects of the occurrence of such breach or violation.
4- Procedures and measures taken, and which implementation is suggested in order to address the mentioned breach or violation and minimize its adverse effects.
5- Breach or violation documentation in addition to the corrective actions adopted.
6- Any other recommendations

In all cases, the Commission shall notify the Data Subject when a breach or violation which prejudices the Data Subject's personal data privacy, confidentiality, and security, as soon as possible. The Commission shall also inform the Data Subject of the procedures they took in this regard.

Article 6: Assigning a Data Protection Officer

The Commission shall assign a Data Protection Officer (DPO) who has the competencies relating to the protection of personal data, and such in any of the following cases:

1- In case the processing operation would cause a highly significant harm on the personal data confidentiality and privacy of the Data Subject as a result of adopting new techniques or techniques which are related to the data volume.
2- In case the processing operation will include a methodical and comprehensive assessment of sensitive personal data, including profiling and automated processing.
3- In case the processing is to be operated on a large volume of sensitive personal data.
4- In case a Data Protection Impact Assessment needs to be run.

The Data Protection Officer may be an employee of the Commission, or whoever is authorized by the Commission, whether by virtue of the Book of Regulations or other means.

The Commission shall determine the contact address of the Data Protection Officer.

The implementing regulation of the present Book determines the types of techniques and standards to determine the volume of required data according to the present Article.

Article 7: Functions of the Data Protection Officer

The Data Protection Officer (DPO) shall be in charge of supporting the Commission's compliance with the enforcement of the provisions of the present Book and its implementing regulation, as well as the instructions issued by the Commission. The DPO shall particularly be in charge of the following tasks and powers:

1- Verifying the quality and correctness of the procedures applied by the Commission.

2- Receiving the requests and claims relating to personal data as per the provisions of the present Book.
3- Providing technical consultations relating to the procedures of periodic assessment and test of the Commission's personal data protection systems and data breach prevention systems, in addition to documenting such assessment results and providing adequate instructions relating thereto, including risk assessment procedures.
4- Acting as focal point within the Commission, as the case may be on the enforcement of the personal data processing provisions stipulated herein.
5- Support the Commission when carrying out a Data Protection Impact Assessment.
6- Any other tasks or powers determined in the present Book.

The DPO shall maintain confidentiality of information and data they receive when performing their tasks and exercising their powers according to the present Book and as per the Commission laws and regulations.

Article 8: Commission's Obligations Towards the Data Protection Officer

The Commission shall provide all means to guarantee that the DPO performs the functions and tasks assigned thereto and provided in Article /7/ of this Book, as required, notably regarding the following:

1- Guaranteeing that the DPO be adequately involved, at the appropriate time, in all matters relating to the protection of personal data.
2- Guaranteeing that the DPO be provided with all required resources and support to carry out the tasks assigned to them.
3- Not terminating the services of the DPO nor imposing a disciplinary sanction for a reason relating to their tasks performance as per the present Book.
4- Guaranteeing not to assign to the DPO any tasks which cause conflict of interests with the tasks assigned to them herein.

The Data Subject may directly contact the Commission according to its adopted procedures regarding the Data Subject personal data and their processing in order to enable them to exercise their rights according to the present Book.

Article 9: Right of the data subject to Access Information

The Data Subject may, based on a written request submitted to the Commission, according to its own procedures, and without any counterpart, access the following information:

1- Types of the Data Subject's personal data which is being processed.
2- Processing purposes.
3- Decisions made based on automated processing, including profiling.
4- Target sectors or facilities with which the Data Subject's personal data will be shared, within and across borders.
5- Regulations and standards for periods of personal data storage and maintenance.
6- Procedures used to correct, remove, or limit the processing operation, in addition to procedures to object on their personal data.

7- Protection measures relating to cross-border processing carried out according to Article 2.2.of this Book.
8- Procedures to be taken in case of breach or violation of the Data Subject's personal data, notably when such breach or violation directly and gravely endangers the privacy and confidentiality of their personal data.
9- Method to submit a request to the Commission.

In all cases, the Commission shall, before starting the processing, provide the Data Subject with the information stipulated in /1/, /2/, /4/, and /7/ of Paragraph /1/ of this Article.

The Commission may refuse the Data Subject's request to access information mentioned in Paragraph /1/ of this Article, when they establish the following:

1- The claim is not related to the information mentioned in Paragraph /1/ of this Article or is excessively repeated.
2- The claim may adversely affect the Commission's efforts to protect information security.
3- The claim may adversely affect the Commission efforts to reveal the fate of the Missing and Forcibly Disappeared.
4- The claim prejudices the privacy and confidentiality of third parties' personal data.

Article 10: Right to Request Personal Data Transfer

The Data Subject may, based on a written request submitted to the Commission, and according to its own procedures, access their own personal data which was provided to the Commission for processing, and such in an organized and machine-readable manner,

The Data Subject may request the transfer of their personal data to another party when such transfer is technically possible and does not contradict the Commission efforts to reveal the fate of the missing and forcibly disappeared.

Article 11: Right to Correct or Remove Personal Data

The Data Subject may, based on a written request submitted to the Commission, and according to its own procedures, request the correction of inaccurate personal data or completion thereof in the Commission's data without any unjustified delay.

The Data Subject may request the removal of their own personal data in the Commission's data in any of the following cases:

1- Their personal data is no longer necessary for the purposes for which it was collected and processed.
2- Their renunciation from the consent on which the processing operation was based.
3- Their objection to the processing or the absence of any legitimate reasons for the Commission to proceed with the processing operation.
4- Their personal data processing was carried out in violation of the present Book and applicable legislations and such removal is necessary to comply with the adopted legislations and standards applicable in this regard.

Except when the legal basis for processing the data is the consent of the data subject, the Commission may refuse deletion of the data if the continuation of processing the personal data is necessary to clarify the fate or the whereabouts of the missing person, or is necessary for historical, statistical and scientific purposes and only in accordance with the conditions set out in Article 2.2.3.

Article 12: Right to Restrict and/or halt Processing

The Data Subject may require the Commission to restrict and/or halt the processing through a written request in any of the following cases:

1. The Data Subject's objection to their personal data accuracy. In this case, the processing operation is restricted for a determined period which enables the Commission to verify their accuracy.
2. The Data Subject's objection to their personal data being processed in violation of the agreed purposes.
3. The processing being carried out in violation of the present Book and applicable legislations.
4. When the processing is carried out for direct marketing purposes, including profiling relating to direct marketing.
5. When the processing is carried out for statistical survey purposes.
6. When the processing violates data processing principles and only in accordance with the conditions set out as per Article /2.2.3/ "Personal Data Processing Without the Data Subject's Consent" of this Book.
7. When it is established that such processing endangers the data subject.

The Data Subject may request the Commission to continue preserving their personal data until after the end of the processing purposes.

Notwithstanding the present Article, the Commission may proceed with the Data Subject's personal data processing in any of the following cases and only in accordance with the conditions set out in article 2.2.3:

1- If the processing is limited to storage for historical purpose.
2- If the processing is necessary to serve the public interest and after conducting a risk assessment to ensure that the processing may not create a risk for the Data Subject.
3- If the processing is necessary to the protection of third parties' rights as per the applicable legislations.

In all cases, the Commission shall, when lifting the restrictions set forth in the present Article, notify the Data Subject thereof.

- For the purpose of this Article, restriction means: the marking of stored personal data with the aim of limiting their processing in the future.
- For the purpose of this Article, halting means: cessation of any operations performed on personal data for a defined or undefined duration.

Article 13: Processing and Automated Processing Rights

The Data Subject may object to the Commission, according to its procedures, to the decisions issued as a result of the automated processing, which have legal repercussions and significantly impact the Data Subject, including profiling.

Notwithstanding Paragraph /1/ of the present Article, the Data Subject may not object to the decisions issued as a result of the automated processing in the following cases:

1- When the automated processing is carried out in accordance with the conditions of the contract concluded between the Data Subject and the Commission.
2- When the Data Subject's prior consent on the automated processing was given as per the conditions set in Article /4/ "Data Processing Consent Conditions" of this Book.

The Commission shall apply the adequate procedures and measures to protect the privacy and confidentiality of the Data Subject's personal data in the cases mentioned in Paragraph /2/ of this Article, without harming or prejudicing the Data Subject's rights.

The Commission shall involve the human element to review the decisions resulting from the automated processing based on the Data Subject's request.

Article 14: Communication with the Commission

The Commission shall provide the adequate clear means and mechanisms to enable the Data Subject to communicate with them and request to exercise any of the Data Subject's rights stipulated in the present Book and according to the implementing regulations which may be issued by the Commission.

Article 15: Security of Personal Data

The Commission shall set adequate technical and organizational procedures and measures in order to guarantee applying a data security level which counterbalances the risks accompanying the processing operation as per the best international standards and practices. Such procedures and measures include the following:

1- Personal data encryption and enforcement of the data masking mechanism.
2- Enforcement of procedures and measures which guarantee maintaining the confidentiality, safety, correctness, and flexibility of the processing systems and services.
3- Enforcement of procedures and measures which guarantee the retrieval of and access to personal data on the determined time in case of any actual or technical failure.
4- Enforcement of procedures which guarantee the smoothness of the testing, assessment, and estimation of the technical and organizational measures efficiency, ensuring the processing security.
5- Refraining from using personal emails to transfer information.

6- Carrying out any communication by email, whether internal or external, on a need-to-know basis, whereby personal data shall only be shared with concerned individuals to prevent its dissemination.
7- Remote access to the server and the use of home computers or laptops shall be in compliance with the safety standards as clarified in the information security policy of the Commission, as much as possible.
8- Refraining from using unsecured internet and radio networks to pull, exchange, transfer, or transmit personal data, except for operational necessities.
9- Requiring employees handling personal data to be vigilant when remotely connecting to the Commission's server.
10- Passwords must be secure and saved. Employees shall verify that they properly logged out and closed the browsers.
11- Using mobile devices in safe locations when working, or when in difficult or dangerous circumstances.
12- Refraining from using mobile devices to preserve personal data classified as sensitive. In case this situation is inevitable, sensitive personal data shall be transferred to a database and adequate data safeguarding measures shall be promptly applied.
13- Safeguarding data in a secure location when temporarily using a USB, memory card, and flash drive to safeguard personal data and encrypting the electronic record. Personal data shall be deleted from mobile devices when the need to use such devices to safeguard personal data ceases to exist.
14- Verification by the Information and Communications Technology Officer (ICT Officer) that data retrieval systems and backups are set and applied in a way to include all electronic records. Moreover, the ICT Officer shall verify that the backup operations are carried out periodically, so as to conform to the sensitivity of the personal data.
15- Automating electronic records so as to allow the easy retrieval of data in case the backup operation is difficult, such as in situations of repeated power outages, electronic systems failure, or natural disasters.
16- Requiring the Commission to coordinate with the ICT Officer in order to remove the data, when there is no need for the electronic records.

When assessing the data security level stipulated in Paragraph /1/ of this Article, the following shall be taken in consideration:

1- Risks accompanying the processing operation, including personal data destruction, loss, minor or illegal change, reveal, or unauthorized access whether such data was transferred, stored, or processed.
2- Processing performance costs, nature, scope, and purposes; and the various potential risks on the privacy and confidentiality of the Data Subject's personal data.

Article 16: Personal Data Protection Impact Assessment

The Commission shall run a Data Protection Impact Assessment (DPIA) when processing personal data is likely to create risks for the rights and freedom of the data subject.

In any case, the Commission shall run a DPIA before transferring any data to a third party.

Without prejudice to the nature, scope, and purposes of the processing operation, the Commission shall, before carrying out the processing, make the assessment of the impact of the processing, and such when using any of the new technologies which may endanger the privacy and confidentiality of the Data Subject's personal data.

The assessment of the impact stipulated in Paragraph /1/ of the present Article is necessary in the following cases:

1- Before transferring personal data to a third party.
2- When the processing includes a methodological and comprehensive assessment of the Data Subject's personal aspects which are based on automated processing, including profiling, and which have legal repercussions or may significantly impact the Data Subject.
3- When the processing is to be conducted on a large volume of sensitive personal data.

The assessment stipulated in Paragraph /1/ of the present Article shall include, at least, the following:

1- A clear and methodological explanation of the processing operations proposed for the protection of personal data and the purpose of such processing.
2- An assessment of whether the processing operations are both necessary and adequate for their intended purpose.
3- An assessment of the potential risks to the privacy and confidentiality of the Data Subject's personal data.
4- Procedures and measures proposed to limit the potential risks on personal data protection.

The Commission may carry out one assessment for a group of processing operations which are similar in nature or risks.

The Commission shall ensure that the DPO is involved when assessing the impact of personal data protection.

The Commission shall prepare a list of the processing operation types for which it is mandatory to carry out a personal data protection impact assessment and make such list available to the public on its website.

The Commission shall periodically review the assessment outcomes in order to verify the processing enforcement according to the assessment in case the risks levels accompanying the processing operations changed.

Article 17: Safety Measures

The Commission shall take all technical, professional, and organizational measures, in light of the personal data nature and the risks resulting from their processing, in order to guarantee the data integrity and protection, and prevent exposing them to breach, corruption, damage, or loss, or being accessed by unauthorized persons, and any other illegal data processing operations.

Article 18: Data Protection Breach

The Commission shall address without unjustified delay any breach of data integrity.

The DPO shall support the Commission in order to provide:

(1) A description of the breach and its type.
(2) A description of the potential consequences of the breach.
(3) A description of the procedures taken or to be taken in order to address the breach consequences, mitigate its impact, and protect personal data.

The DPO shall hold a record of all breaches (including, *inter alia*, breaches of data integrity mentioned in Paragraph (1) above, their consequences, and the measures taken to address them).