Procedural Guide to Palestinian Personal Data Protection in the Digital Space

حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

May
2023

7amleh – The Arab Center for the Advancement of Social Media

Procedural Guide to Palestinian Personal Data Protection in the Digital Space

Developed by: Andersen Palestine
Edited and Reviewed by: Cathrine Abuamsha
Ritaj for Managerial Solutions edited the Arabic edition of this guide and translated it into English.
Copyedited by: Yasmeen Iraqi

Contact us:
Email: info@7amleh.org
Website: www.7amleh.org
Telephone: +972 (0)774020670

Find us on social media: 7amleh

7amleh – The Arab Center for the Advancement of Social Media expresses its high thanks to the Palestinian Digital Rights Coalition for its insightful contribution to the review and discussion of the first edition of this guide.

Contents

Introduction

Since 2012, the United Nations Human Rights Council (UHRC) has shined a light on the necessity to enshrine and protect human rights both off- and- online[1]. In its twentieth session, the UHRC affirmed that "the same rights people enjoy offline must also be protected online." In an unwavering resolution, the UN body continues to underline this corpus of rights that became known as digital rights, the entitlements all members of humankind are entitled to enjoy—including the Palestinian people.

7amleh – The Arab Center for the Advancement of Social Media focuses on digital rights in pursuit of a safe, fair, and free digital space for Palestinians, men and women. In doing so, it gears its programs toward monitoring, researching, advocating, and raising awareness about this dimension of human rights, and it places a focus on the right to privacy and the protection of digital personal data—that is the focus of this guide's attention.

The Palestinian context marks a departure from core international human rights conventions and best practices on the right to privacy and digital data protection. This major issue exposes the privacy, security, and other rights of Palestinians to whirlwinds of danger and exploitation—the status quo 7amleh has exerted itself for years to change. The Procedural Guide to Palestinian Personal Data Protection in the Digital Space marks one link in 7amleh's chain of publications and concerted efforts to improve Palestinians' privacy and data protection. Several publications, surveys, online campaigns, and audiences with stakeholders and decision-makers preceded and informed the development of this guide. Along the way, 7amleh arrived at a prominent finding; Palestinians need and support a Palestinian legislation protecting personal data—a position held by 69 percent of respondents.

In a digital age through and through and increasing use of digital data by individuals, communities, governmental agencies, nongovernmental organizations (NGOs), and the private sector, the significant need to protect these data pressingly stand out. Given the rising technological capabilities of governments and corporations, among others, digital data can be attributed to a specific person or entity, accessed, and used for a slew of purposes, including privacy violations.

In the State of Palestine, the right to privacy is a constitutional right guaranteed by the Amended Basic Law of 2003. The State of Palestine also acceded to the International Covenant on Civil and Political Rights, which guarantees the right to privacy both online and offline. Therefore, Palestinians—individuals, governmental agencies, NGOs, and the private sector—are expected to respect and protect privacy in all spaces.

1 United Nations Human Rights Council. A/HRC/RES/20/8. UNHRC Session 20, July 16 2012.
https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement

However, given the novelty of this entitlement and fast advances in technology, there are very few instruments to protect the right to privacy as a basic digital human right by means of digital data protection. The European Union General Data Protection Regulation (GDPR) is the most important instrument that guarantees the right to privacy in the digital space, providing the best data protection standards at all stages of data processing. Therefore, many non-EU parties adopt the GDPR as an ideal reference for privacy protection and respect in the digital space, especially those dealing with European individuals or entities.

In light of the preceding, this reference was created to guide individuals, institutions, and the private sector in the State of Palestine to better protect the right to privacy in dealing with digital data based on Palestinian legislation and International Human Rights Law. Furthermore, it taps into the GDPR[2], to provide the best practices at this forefront.

2 The European Union General Data Protection Regulation (GDPR), 2016/679. https://gdpr.eu/tag/gdpr/.

Why Comply with Privacy Rules?

Individual privacy protection and compliance, including personal information, is critical for several reasons—the most

- Comply with a statutory obligation to respect and protect the right to privacy both online and offline;
- Ensure the safety and security of processing the internet user data toward a safe use of the network; and
- Maintain credibility and transparency to cement the trust of commercial or governmental parties dealing with complying parties.
-

Key Concepts

The GDP³R, identifies the terms below, among others, as key concepts that must be carefully considered for proper personal data processing:

- 'personal data' means any information relating to an identified or identifiable natural person.
- 'data subject' means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to their personal data, such as

3 GDPR, Article 1.4. https://gdpr.eu/article-4-definitions/.

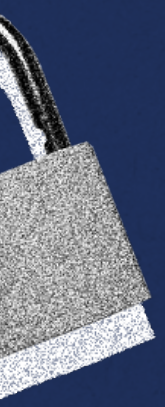
In addition, the data subject may be identified in reference to the name, identification number, or to one or more factors specific to that natural person's physical, mental, economic, or social identity.

The data subject can be directly identified if it is possible to identify them through one piece of information from one party, such as their name. The indirect method involves collecting data from different sources and piecing them together to construct a specific corpus of information about a particular person, such as gender or date of birth.

- 'Sensitive personal data' means personal data that is considered more sensitive than normal personal data and causes greater harm to the data subject if breached. This category includes data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation.

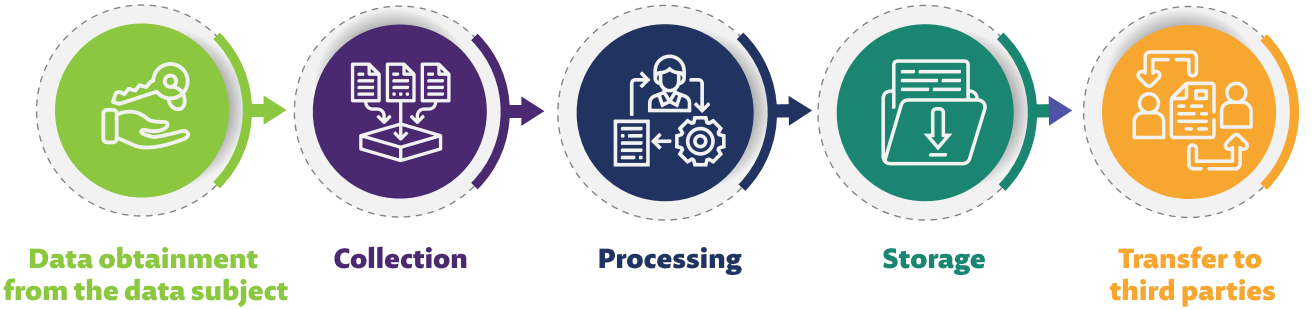
1. 'Controller' means the natural or legal person, alone or jointly with others, collects and processes data and determines the purposes and means of collection.
2. Government: The government collects and processes citizens' data for several reasons, including public sector governance, public service provision, archiving, and statistics.
3. Private Sector: Private firms and establishments collect and process individual data for several reasons, including app/web user experience improvement, service provision, and marketing.
4. Institutions: Companies/ organizations collect and process individual data for several reasons, including adding new customers/ users to their website to mailing lists and improving website user experience.

- 'Processor' means a natural or legal person who processes personal data on behalf of the controller.
- 'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, or behavior.
- 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.



What are the Operations Performed on Data in the Digital Space?

In the digital space, data may go through several operations that could be summed up as follows:



- Obtainment: In this case, the data subject provides their data voluntarily to the controller (e.g., when the user provides their name and email to a website to subscribe to its mailing list).
- Collection: This mechanism involves the obtainment of data on a particular person or entity, either by requesting them from the data subject or collecting it automatically.
- Processing: This course of action involves an 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, use, erasure or modification.

In most cases, the controller is also the processor; in others, the former assigns the processing to another party. The controller may act as is with a specific set of data and as a processor with other data.

Data Collection and Processing Principles

The following principles should guide data collection and processing in accordance with national and international standards:

- Lawfulness, Fairness, and Transparency: As this principle stands, data needs to be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Along the same lines, the data subject must be aware that their data are used and processed. Compliance with this principle also requires that

1. Any information and communication relating to the processing of those personal data be easily accessible by the data subject and easy to understand, and that clear and plain language be used.
2. Natural persons should be made aware of risks, implications, and rights in relation to the data collection and how to exercise their rights in relation to such operations.
3. The information addressed to the public or the data subject should be presented in brief, accessible, plain language. To this end, illustrations or graphics may be used as needed, especially where there are multiple parties and technologies, which might make it difficult for the data subject to know the collector and collection purposes (e.g., advertisement).

- Purpose Limitation: The data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or research purposes, or statistical purposes must not be considered to be incompatible with the initial purposes, provided no arbitrary power is exercised under the pretense of public interest.
- Data Minimization: Data collection and processing should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. And data should not be collected unless the purpose of the processing cannot reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.
- Accuracy: The collected data must be accurate and, where necessary, kept up to date; every reasonable step 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 without delay. In the same vein, every reasonable step is to be taken to ensure the security and confidentiality of the data, including preventing any breach or unauthorized access to or use.

Data Collection and Processing Legal Bases

Any legislation on data collection and processing should be steeped in the following key pillars:

- There must be provisions that allow or impose the collection and processing of data so that data are collected and processed
  1. according to applicable provisions, provided that these provisions be clear and precise and their application should be foreseeable to persons subject to it;
  2. to comply with a legal obligation to which the controller is subject for performing a task in the public interest or exercising official authority vested in the controller, provided this is not used to justify abuse of power[4].
- Data should be allowed when necessary to protect the vital interests of the data subject or of another natural person.

Data collection and processing should also be regarded as lawful where it is necessary to protect an interest that is essential for the life of the data subject or that of another natural person. Collection and processing of personal data based on the vital interest of another natural person should, in principle, take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject, for instance, when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, particularly in situations of natural and man-made disasters, provided such circumstances not be used as a pretence for arbitrary collection and processing of data.

- Data processing should be carried out if necessary for the purposes of legitimate interests.
- Data processing may be pursued to serve the legitimate purposes of a controller or another party, provided that the purposes or the fundamental rights and freedoms of the data subject and applicable legal basis are not overriding and that the data are protected. These aims include but are not limited to:
  1. Corruption prevention,
  2. Network safety,
  3. Identification of actus rei or criminal threats to public order—in this case, the processing decision is to be taken by a neutral party.
- Data processing may be carried out if necessary for the performance of a contract;

Data processing may be carried out if necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract.

- Data processing may proceed if the data subject has given consent to the collection of their data

This situation is most common and often devised in individual data processing cases.
sing cases.

4 According to Decree No. 10 of 2018 on Cybercrime, the service provider, The service provider, who is defined as a person who offers its service users the ability to communicate via information technology or any other person who processes, stores, or hosts computer data on behalf of any electronic service provider or users must provide the competent authorities with the user information to help uncover the truth, at the request of the Public Prosecution or competent court. It must also keep the user information for no less than three years, including the user information held by the service provider about the type of telecommunications service, technical conditions, service period, user›s identity, postal or geographical address or telephone, payment information available based on the service agreement or installation, and any other information about the installation location of the communication equipment based on Service Agreement. Moreover, as article 33 of the same decree stands, the public prosecution may obtain the devices, tools, means, electronic data or information, traffic data, data relating to communication traffic or users, or relevant user information in relation to the cybercrime.

Consent Definition

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes; thereby, they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating thereto.

Conditions for Consent

1. **Consent must be a clear affirmative statement. This means that implicit consent must not be considered, and the data subject must take affirmative action to assert their consent to the collection and processing of their data, such as**
   - Written statement of consent, including by electronic means
   - Oral consent
   - Ticking a box on an internet website
   - Choosing technical settings for information collection or another statement or conduct that clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data
   - Consent must not be valid unless expressed by a certain action or motion; thus, silence, pre-ticked boxes, or inactivity should not, therefore, constitute consent
   - For children under 16, data collection is lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the children. Notwithstanding, this condition should not apply to private firms that provide services for adults only and are not offered for children in any way, shape, or form
   - While there is no standard consent form, the written statement is preferable so that the collector and controller may refer to it as needed
2. **Consent should be freely given. This means that the data subject has expressed their conviction, wishes, and agreement to the processing of their data without any pressure that might have influenced their decision.**
   - When assessing whether consent is freely given, utmost consideration must be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
   - If the data subject's consent is given in the context of a written declaration that also concerns other matters, the request for consent has to be presented in a manner that is clearly distinguishable from the other matters in an intelligible and easily accessible form, using clear and plain language.
   - If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
   - Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.
3. **Consent must be based on clear information:**

The data provided to the data subject must answer the following questions:

- Who is the collector?
- What is the collected data?
- Why are these data collected, and for what purpose(s)?

4. Consent must be specific and for certain legitimate purposes:

- Consent must be specific and for specific purposes. These pursuits must be clear and adequately explained to the data subject, and the power of the collector and controller should be limited to the purposes to which the consent has been freely given.
- When the data collection process takes place for multiple purposes, the data subject's consent must be obtained for each purpose.
- As for the burden of proof and requirements for consent, where processing is based on the data subject's consent, the processor should be able to demonstrate that the data subject has given written consent to the processing operation, including ensuring that—
- the data subject is aware of the fact that ant the extent to which consent is given;
- the data subject consent is obtained to an intelligible and easily accessible privacy policy using clear and plain language free of any unfair terms.

Rights of the Data Subject

This section moves to the set of rights entitled to the data subject.

1. Right of access by the data subject

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and a copy thereof, including—

- Processing purposes;
- Personal data categories in question;
- The recipients or categories of recipients to whom the personal data have been or will be disclosed;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with a supervisory authority;
- Where the personal data are not collected from the data subject, any available information as to their source;
- The automated processing procedures.

2. Right to rectification

- The data subject has the right to obtain from the controller the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject should also be entitled to have incomplete personal data completed, including by means of providing a supplementary statement.

3. Right to erasure ('right to be forgotten')

- The data subject has the right to cause the controller to erase their personal data concerning without undue delay, and the controller should be expected to erase personal data without undue delay where one of the following grounds applies

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- The data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- The data subject objects to the processing of their data;
- The personal data have been unlawfully processed;
- The personal data have to be erased for compliance with a legal obligation.

- Where the controller has made the personal data public, yet the data subject made a request to erase their data. In this case, the controller should take reasonable steps, including technical measures, to inform controllers who are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
- Notwithstanding, the right to be forgotten should be suspended to the extent that processing is necessary for the following:
  - Exercising the right of freedom of expression and information;
  - Reasons of public interest in relation to public health (e.g., epidemic prevention and control);
  - Archiving purposes in the public interest, scientific or historical research purposes; or
  - The establishment, exercise, or defence of legal claims.

4. Right to restriction of processing

- The data subject has the right to restrict the processing of their data where one of the following applies:
  - 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;
  - The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  - The controller no longer needs the personal data;
  - The data subject has objected to processing pending the verification of whether the legitimate grounds of the controller override those of the data subject.
- Where processing has been restricted, such personal data should, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise, or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.
- A data subject who has obtained a restriction of processing needs to be informed by the controller before the restriction of processing is lifted.

5. Right to data portability

- The data subject has the right to receive the personal data concerning them in a structured, commonly used and machine-readable format and may transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
  - The processing is based on consent on a contract; and
  - The processing is carried out by automated means.
- In exercising their right to data portability, the data subject are entitled to have the personal data transmitted directly from one controller to another, where technically feasible.
- This right must not be exercised if the processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller on behalf of competent authorities.

6. **Right to object**

- The data subject has the right to object, on grounds relating to their particular situation, at any time to the processing of personal data concerning them, which is based on
  - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
  - Processing is necessary for the purposes of the legitimate purposes pursued by the controller or by a third party.
- In this case, the controller must not process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise, or defence of legal claims.
- Where the data subject objects to processing for direct marketing purposes, the personal data must no longer be processed for such purposes.

7. **Right to an effective judicial remedy against the collector(s), processor(s). In the event of a personal data breach, be it online or offline, the governmental agencies and supervisory authorities entrusted with its protection must adopt and impose deterrent penalties commensurate with the extent of the damage.**
8. **Right to compensation and liability**

What Are the Controller's Responsibilities?

This section is given over to the main responsibilities entrusted to data controllers in relation to personal data processing.

A. Empower the data subject to exercise their rights, including

- Ensuring simple, easy access to information without unreasonable effort on the part of the data subject and when the data subject lodges a request to exercise any of their rights:
  - The data controller must inform the data subject of the actions taken at their request and must respond to the request in the same manner in which the request was submitted. For example, where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information must be provided in a commonly used electronic form.
  - If the data controller does not take any action regarding the request submitted by the data subject, it must inform them of that within a reasonable period.
  - All information related to requests must be provided free of charge; however, the controller may, after demonstrating that a request is manifestly unfounded or excessive, in particular, because of their repetitive character (i.e., received more than three times), the controller may either charge a fee for providing the information or communication or refuse to act on the request.
  - Where the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

B. Provide the data subject with information about their data processing.

- Where personal data relating to a data subject are collected from the data subject, the controller is expected, when personal data are obtained, provide the data subject with all of the following information:

- The identity and contact details of the controller and, where applicable, of the controller's representative;
- The contact details of the data protection officer;
- The purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;
- The recipients who will access the information;
- Where applicable, the fact that the controller intends to transfer personal data to a third country must be communicated to the data subject.

- The data collector must, when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
  - The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
  - Their right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to the processing as well as the right to data portability;
  - Their right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
  - Their right to lodge a complaint with a supervisory authority;
  - Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and of the possible consequences of failure to provide such data;
  - The existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller must provide the data subject prior to that further processing with information on that other purpose and with any further relevant information about the further purpose.

C. Comply with the lawful procedure of data processing.

- Given the nature and purpose of data processing and the high risks to individual rights and freedoms and rights, the data controller must ensure that all steps are taken to ensure that the data processing process is carried out in accordance with the law.
- Where two controllers jointly determine the purposes and means of processing, they determine their respective responsibilities for compliance with the legal obligations in relation to data processing.

D. Notification of a personal data breach to the supervisory authorities and individuals.

- In the case of a personal data breach, the controller must, without undue delay and, where feasible, not later than seventy-two hours after having become aware of it, notify the supervisory authority competent of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within seventy-two hours, it must be accompanied by reasons for the delay, including:
  - A description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  - The name and contact details of the data protection officer or another contact point where more information can be obtained;
  - A description of the likely consequences of the personal data breach;
  - A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including those to mitigate its possible adverse effects.

- When the personal data breach is likely to affect the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subject without undue delay to enable them to take necessary precautionary measures. The communication must describe the nature of the personal data breach and the proposed measures to be taken to mitigate the adverse impact of the breach. Besides, it must contain at least the following information:
  - The name and contact details of the data protection officer or another contact point where more information can be obtained;
  - A description of the likely consequences of the personal data breach;
  - A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including those to mitigate its possible adverse effects.
- The notification of a personal data breach to the data subject must not be required if any of the following conditions are met:
  - The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption.
  - The controller has taken subsequent measures which ensure that the risk to the rights and freedoms of data subjects is no longer likely to materialise.
  - It would involve a disproportionate effort. In such a case, there has to be instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

E. Recording of processing activities.

- Each controller must maintain a record of processing activities, including—
  - The name and contact details of the controller;
  - 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 have been or will be disclosed;
  - Transfers of personal data to a third country;
  - The time limits for the storage of the different categories of data;
  - A general description of the technical and organizational security measures to maintain information confidentiality.

What Is the Difference If the Controller Assigns Processing to Another Party?

- Where the controller assigns processing to another party, the controller must use only processors providing sufficient guarantees to implement appropriate technical and organizational measures and ensure the protection of the rights of the data subject.
- Processing by a processor other than the controller must be governed by a written 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 the obligations and rights of the controller.

- The assigned processor must process the personal data based on documented instructions from the controller.
- The processor is not allowed to communicate data with a third party without the controller's prior written authorization.

The Obligations of Assigned Processors

The assigned processor is expected to:

1. **Maintain a record of processing activities;**

Each processor must maintain an archive or a record of all processing activities.
The record should include the following:

- The name and contact details of thereof (i.e., processor) and of each controller on behalf of which the processor is acting;
- The categories of processing carried out on behalf of each controller;
- Where applicable, transfers of personal data to a third country, including the identification of that third country or international organization;
- A general description of the technical and organizational security measures devised to protect information confidentiality.

2. **Maintain data security and confidentiality in processing;**

Taking into account the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller, and the processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The pseudonymization and encryption of personal data to avoid the misuse thereof to identify natural persons;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Parties involved in data processing must ensure that any natural person acting under their authority and having access to personal data does not process it unless instructed to do so by their employer.

3. **Notify, without any undue delay, the controller of any personal data breach.**

Cases and Scenarios

This section presents some common cases and scenarios for data collection and control operations. Human rights principles and best international practices, including personal data protection regulations, must underpin all of these activities. And the rights of data subjects should be respected and guaranteed, as illustrated throughout the various sections of this guide.

A. Case No. 1: Governments as Data Controllers and Processors

For governments to deliver services to their citizens, as the Palestinian government does through its bodies and ministries (e.g., Ministry of Interior, Ministry of Foreign Affairs, Ministry of National Economy (MoNE), Ministry of Justice, and Ministry of Labor), the members of the public must provide certain information about themselves. For example, to register a company with the MoNE, the latter requests a set of information, including but not limited to partners' identities, addresses, and the articles of association.

B. Case No. 2: Banks as Data Controllers and Processors

To open a bank account, the bank requests a slew of personal information and data. Once the account is open, the bank retains knowledge and control over the client's account information. In layman's terms, the bank controls and processes its clit data.

C. Case No. 3: The Private Sector as a Data Controller and Processor

Some private sector firms demand an assortment of personal data from their customers to authenticate their identity, inform legitimate marketing activities, and boost service quality and customer experience. For example, insurance firms demand a mine of data from their clients in order to determine the best insurance plan for them. To assign a phone number and deliver associated services, telecommunications firms and service providers also need numerous pieces of personal information from subscribers. In all of these instances and others, the private sector acts as the controller and processor of its diverse pool of customer data.

D. Case No. 4: Smart Applications and Websites as Data Controllers and Processors

Governments, NGOs, and the private sector use websites and smart applications to ensure the speed and ease of their modus-operandi. If data is amassed and processed, whether automatically or manually, the entity that owns or operates these websites or applications serves as the data controller, processor, or both.

By and large, all entities that own, operate, or both own and operate applications or websites must post on their terms of use and privacy policies to assert the lawfulness of data collection, processing, and storage.

حملة – المركز العربي
لتطوير الإعلام الاجتماعي

7amleh - The Arab Center for
the Advancement of Social Media