EU Twinning Project on
Statistics in Jordan

دائرة الإحصاءات العامة
Department of Statistics

# General introduction to General Data Protection Regulation (GDPR)

## Activity 1.4.6:
## Security policy and data confidentiality

**Amman, 8th January 2024**

# Agenda

- Statistical secret vs Privacy
- How «privacy» is regulated
- GDPR - some definitions
- Who is involved in processing personal data
- Data Protection Officer
- Istat experience
- Privacy and official statistics: is it a possible combination?

# Statistical secret vs Privacy

- **Statistical secrecy** is a provision aimed at increasing the **quality** of statistical information by eliminating the convenience of opportunistic behavior on the part of those who have to provide statistical data.
- So, the primary purpose is not to protect privacy, but increase trust in respondents.
- In Italy, statistical secret was born in 1894 with Royal Decree and is nowadays regulated by Law 322/1989 art. 9. Statistical secret is not applied at public data or well known data
- In Jordan?

# Statistical secret vs Privacy

- **Privacy** doesn't mean today the "right to be alone", as originally thought, but **personal data protection** and, in particular, the right of the person to control that the information concerning him is treated or viewed by others only in case of need.
- **Privacy** is a much broader concept than statistical secrecy.

# How «privacy» is regulated

- In 2016 the EU Regulation 2016/679 (so called General Data Protection Regulation - GDPR) was released. In 2018 was adopted in all european countries.
- Before, we had the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- The GDPR must be read also with specific privacy code adopted in each country. In Italy the privacy code is the Law 196/2003.
- In Jordan?

# How «privacy» is regulated

- To understand the impact on official statistics, we have to consider that EU Regulation 2016/679 required public and private organizations to review their organizational structure, considering the **centrality** of the confidentiality and protection of personal data.

# GDPR - some definitions

- '**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- '**genetic data**' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

# GDPR - some definitions

- '**biometric data**' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- '**data concerning health**' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

# GDPR - some definitions

- '**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;
- '**restriction of processing**' means the marking of stored personal data with the aim of limiting their processing in the future;

# GDPR - some definitions

- '**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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

# Who is involved in processing personal data

ACTIVE SUBJECTS

- '**Controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- Controller is **accountable** for each 'processing' so for any operation or set of operations which is performed on personal data or on sets of personal data and has to be able to demonstrate compliance with GDPR principles

# Who is involved in processing personal data

- '**Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

PASSIVE SUBJECTS

- '**Data subject**' is the person who personal data are referred

# Data Protection Officer

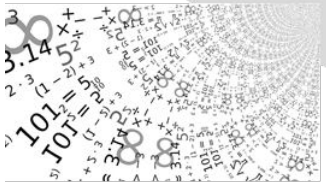
- In case of National Institute of Statistics, the controller and the processor shall designate a data protection officer and shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

# Data Protection Officer

- The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
- The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

# Istat experience

**Statistical production**



Istat | Istituto Nazionale di Statistica

**Administrative and management activity**

Delegation of the European Union to Jordan

TWINNING

دائرة الإحصاءات العامة
Department of Statistics

STATISTICS DENMARK

DESTATIS
Statistisches Bundesamt

Istat

STATISTICS LITHUANIA
STATE DATA AGENCY

Statistics Finland

# Statistical production… like a steeplechase

Applying the principles of **privacy by default and by design** to all stages of statistical processing can be perceived as a steeplechase, in which it is necessary to continually balance the need to produce official statistics with the protection of confidentiality of data subjects

Delegation of the European Union to Jordan
TWINNING
دائرة الإحصاءات العامة
Department of Statistics
STATISTICS DENMARK
DESTATIS
Statistisches Bundesamt
Istat
STATISTICS LITHUANIA
STATE DATA AGENCY
Statistics Finland

# Privacy by design and privacy by default

- The term **privacy by design** means nothing more than “data protection through technology design”.
- In other words, data protection is better guaranteed when it is already integrated in the technology at the moment that is created. Nevertheless, there is still uncertainty about what “Privacy by Design” means, and how one can implement it.  Legislation leaves completely open which exact protective measures are to be taken.
- **Privacy by default** means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy friendly ones (minimization of personal data)

# Privacy Impact Assessment

- The instrument for a privacy impact assessment (PIA) or data protection impact assessment (DPIA) was introduced with the Art. 35 of the GDPR. This refers to the obligation of the controller to conduct an impact assessment and to document it before starting the intended data processing. One can bundle the assessment for several processing procedures.
- Basically, a data protection impact assessment must always be conducted when the processing could result in a high risk to the rights and freedoms of natural persons.

# Privacy Impact Assessment

- The assessment must be carried out especially in case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in art. 9, or of personal data relating to criminal convictions and offences referred to in art. 10;

(c) a systematic monitoring of a publicly accessible area on a large scale.

# Privacy Impact Assessment

- In order to specify exactly in which cases a privacy impact assessment has to be performed, the supervisory authorities are involved.
- Taking into consideration that NSIs have appointed a Data Protection Officer, his advice must be taken into account when conducting a DPIA.
- How and by what criteria the consequences and risks for the data subjects are assessed, remains largely unanswered.

# Privacy Impact Assessment

- **How to conduct a DPIA?**

- Istat released a template divided into 3 sections:

1) Statistical process description
2) Compliance with GDPR principles
3) Risk analysis

# GDPR principles

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘**lawfulness**, **fairness** and **transparency**’);
- 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 historical research purposes or statistical purposes shall, in accordance with art. 89, not be considered to be incompatible with the initial purposes (‘**purpose limitation**’);

# GDPR principles

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimization**’);
- 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 (‘**accuracy**’);

# GDPR principles

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with art. 89 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘**storage limitation**’);

# GDPR principles

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality**’).
- The controller shall be responsible for, and be able to demonstrate compliance with principles (‘**accountability**’).

# Risk assessment (ENISA approach)

- **Risk = Likelihood x Impact**
- What's Likelihood? **Threats x Vulnerabilities**
- The assessment of risks is the first step towards the adoption of appropriate security measures for the protection of personal data, in order to guarantee confidentiality, integrity, availability of data

- https://www.enisa.europa.eu/risk-level-tool/risk

# Risk assessment (ENISA approach)

- The main steps are:
- *Definition and Context of the Processing Operation*
- This step is the starting point of the risk assessment and is fundamental in order to define the boundaries of the data processing operation (under assessment) and its relevant context. In doing so, the organization needs to consider the different phases of the data processing (collection, storage, use, transfer, disposal, etc.) and their subsequent parameters.

# Risk assessment (ENISA approach)

- *Impact evaluation*
- Based on the analysis of previous step, the data controller/processor at this stage must assess the impact on the fundamental rights and freedoms of the individuals, resulting from the possible loss of security of the personal data. Four levels of impact are considered (Low, Medium, High, Very High)

# Risk assessment (ENISA approach)

| LEVEL OF IMPACT | DESCRIPTION |
|---|---|
| Low | Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.). |
| Medium | Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.). |
| High | Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.). |
| Very high | Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.). |

# Risk assessment (ENISA approach)

- *Threat Analysis*
- A threat is any circumstance or event, which has the potential to adversely affect the security of personal data. At this step, the goal for the data controller/processor is to understand the threats related to the overall environment of the personal data processing (external or internal) and assess their likelihood (threat occurrence probability). Varying levels and types of threats to the confidentiality, integrity and availability of personal data could be considered in this respect.

# Risk assessment (ENISA approach)

- Three levels of threat occurrence probability are defined, namely:
- **Low**: the threat is unlikely to materialize.
- **Medium**: it is possible that the threat materializes.
- **High**: the threat is likely to materialize.

# Risk assessment (ENISA approach)

- To simplify the process the ENISA's approach defines four areas of assessment for threat occurrence probability and guides the controller through them, namely:

- Network and technical resources (hardware and software)

- Processes/Procedures Related to the Processing of Personal Data

- Different parties and people involved in the processing operation

- Business sector and scale of the processing

- At the end, the threat occurrence probability is obtained as the highest of the scores obtained per area.

# Risk assessment (ENISA approach)

- *Risk evaluation*
- After evaluating the impact of the personal data processing operation and the relevant threat occurence probability, the final evaluation of risk is possible as shown.

# Risk assessment (ENISA approach)

- *Security Measures*
- It should be noted that the adequacy of measures to specific risk levels should not be perceived as absolute. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk.

# Which rights for data subjects?

- *Right of Access*
- The right of access plays a central role in the GDPR. On the one hand, because only the right of access allows the data subject to exercise further rights (such as rectification and erasure). On the other hand, because an omitted or incomplete disclosure is subject to fines.
- The answer to a right of access request includes two stages. First, the controller must check whether any personal data of the person seeking information is being processed at all. In any case, one must report a positive or negative result.

# Which rights for data subjects?

- If the answer should be positive, the second stage involves a whole range of information (e.g.: processing purposes, categories of personal data processed, recipients or categories of recipients, the planned duration of storage or criteria for their definition, information about the rights of the data subject such as rectification, erasure or restriction of processing, information about the origin of the data, as long as these were not collected from the data subject himself, and any existence of an automated decision-taking process, including profiling, with meaningful information about the logic involved as well as the implications and intended effects of such procedures. Last but not least, if personal data is transmitted to a third country without an adequate level of protection, data subjects must be informed of all appropriate safeguards which have been taken.

# Which rights for data subjects?

- *Right to be Forgotten*
- The right to be forgotten derives from the case Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González (2014). For the first time, the right to be forgotten is codified and to be found in the GDPR in addition to the right to erasure.
- When it is possible to exercise this right, personal data must be erased immediately where the data are no longer needed for their original processing purpose, or the data subject has withdrawn his consent and there is no other legal ground for processing, the data subject has objected and there are no overriding legitimate grounds for the processing, or erasure is required to fulfil a statutory obligation under the EU law or the right of the Member States.

# Which rights for data subjects?

- *Right to be Forgotten*
- In addition, data must naturally be erased if the processing itself was against the law in the first place.

# Which rights for data subjects?

- *Right to be Informed*
- There is a need for transparency regarding the gathering and use of data in order to allow EU citizens to exercise their right to the protection of personal data. Therefore, the GDPR gives individuals a right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller.
- The law differentiates between two cases: On the one hand, if personal data is directly obtained from the data subject (Art. 13 of the GDPR) and, on the other hand, if this is not the case (Art. 14 of the GDPR).

# Which rights for data subjects?

- *Right to be Informed*
- Where data is obtained directly, the person must be immediately informed, meaning at the time the data is obtained. In terms of content, the controller's obligation to inform includes his identity, the contact data of the Data Protection Officer (if available), the processing purposes and the legal basis, any legitimate interests pursued, the recipients when transmitting personal data, and any intention to transfer personal data to third countries.

# Which rights for data subjects?

- In addition, the right to be informed also includes information about the duration of storage, the rights of the data subject, the ability to withdraw consent, the right to lodge a complaint with the authorities and whether the provision of personal data is a statutory or contractual requirement. In addition, the data subject must be informed of any automated decision-making activities, including profiling. Only if the data subject is already aware of the above information it is not necessary to provide these.

# Which rights for data subjects?

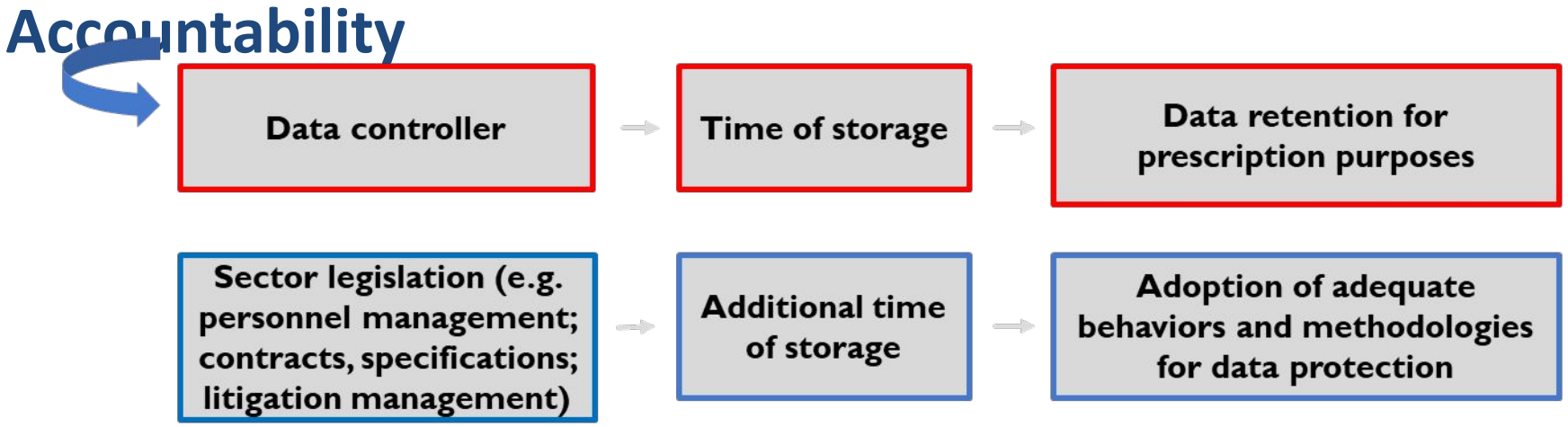
- If personal data is not obtained from the data subject, he or she must be provided the information within a reasonable period of time, but at latest after a month. In cases where the gathered information is used to directly contact the data subject, he or she has the right to be informed immediately upon being approached. As far as content is concerned, the controller has to provide the same specific information as if the personal data would have been directly obtained from the data subject.

# Fines / Penalties

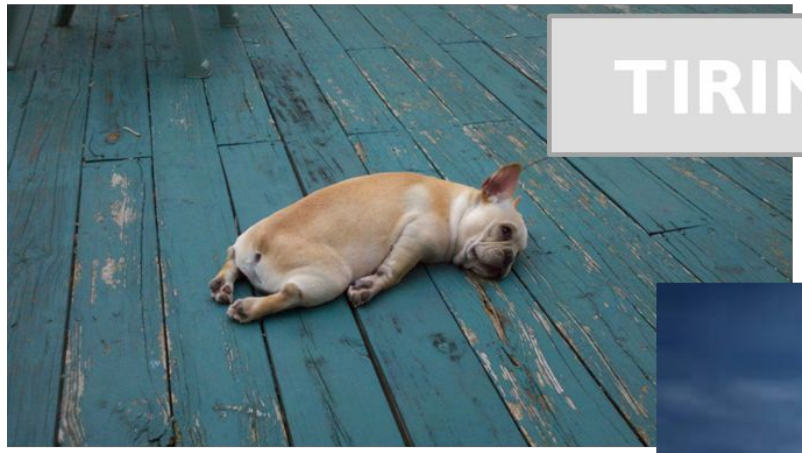
- National authorities can or must assess fines for specific data protection violations in accordance with the GDPR. The fines are applied in addition to or instead of further remedies or corrective powers, such as the order to end a violation, an instruction to adjust the data processing to comply with the GDPR, as well as the power to impose a temporary or definitive limitation including a ban on data processing. For the provisions which relate to processors, he may be subject to sanctions directly and/or in conjunction with the controller.

# Administrative and management activity

- Pay attention to whistleblowing and online selection… DPIA is required!
- Storage limitation «… personal data may be stored for longer periods insofar as the personal data will be processed…»



# Privacy and official statistics: is it a possible combination?





EU Twinning Project on
Statistics in Jordan

دائرة الإحصاءات العامة
Department of Statistics

# Thank you for your attention and support