



Electricity
Authority
of Cyprus

EADPP european association
of data protection
professionals

Legal and practical GDPR Challenges and Opportunities during the COVID-19 pandemic: Electricity Authority of Cyprus an example



26 November 2020

EADPP Annual Conference 2020

Maria Kyprianou, EADPP Branch Cyprus

Legal Services Officer & DPO Electricity Authority Cyprus

Contents

- 1. Introducing the COVID-19 GDPR Challenge**
- 2. EAC Response to COVID-19**
- 3. GDPR Compliance Obligations**
 1. The Data Protection Principles
 2. The rights of Data subjects
 3. GDPR Procedures
- 4. Recommendations & Opportunities**



1. Introducing the COVID-19 GDPR Challenge



1. Introducing the COVID-19 GDPR Challenge

2012 - 2016

Discussions for protecting data
subject's rights

25th May 2018

GDPR 2016/679

**GDPR
2016/679**

Challenges and opportunities
for companies, organisations
and Governmental entities



1. Introducing the COVID-19 GDPR Challenge



1. Introducing the COVID-19 GDPR Challenge

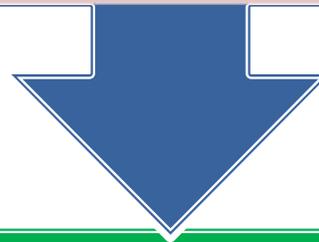
**Companies and other entities set the foundations for
A safer data environment.**



1. Introducing the COVID-19 GDPR Challenge

March 12th 2020...

the World Health Organisation announced the COVID-19 outbreak A
PANDEMIC!



Everyday life as we know it changed dramatically.



1. Introducing the COVID-19 GDPR Challenge

Covid-19

Protective measures affecting privacy and data protection by Governments

Additional challenges to companies towards their customers, personnel, stakeholders and the society at large.



1. Introducing the COVID-19 GDPR Challenge

What is the BIG COVID-19 Challenge?

Now companies must

- **continue implementing their GDPR compliance Policies,**
- **but also abide by COVID-19 legislation in line with their Risk Assessment Strategy.**



1. Introducing the COVID-19 GDPR Challenge

Today's Objectives

Present the Electricity Authority of Cyprus COVID-19 response

Examine the GDPR obligations, alongside the COVID-19 protective measures

Provide Recommendations and Opportunities through practical examples.

Long-Term Objectives

Implement, evaluate, re-design, re-implement and re-evaluate measures and solutions that

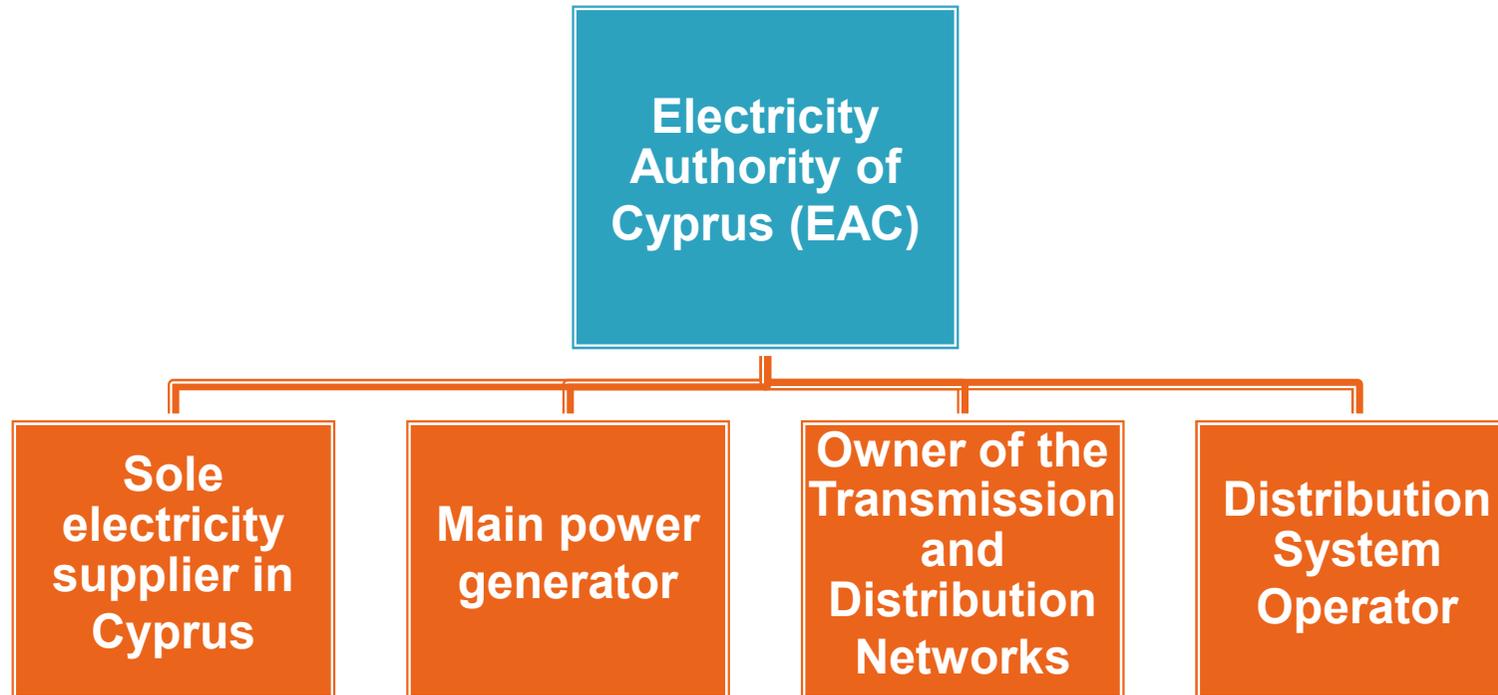
- Respect the rights of data subjects,
- Strike a balance with the obligation to protect society
- Create new business opportunities.



2. EAC Response to COVID-19



2. EAC Response to COVID-19



2. EAC Response to COVID-19

EAC is an Essential Service for the operation of the state and it cannot stop supplying electricity.

As an employer and as a business EAC owes a duty of care towards:

- its employees,
- its customers
- its associates and
- the society.



2. EAC Response to COVID-19



- EAC appointed the **Covid-19 Task Force** to study and design the necessary actions and measures.
- **EAC Managers** have the responsibility to implement the measures.
- All actions and measures decided follow **Government guidance** and protect public interest and health.
- **Employees are informed** through Circulars that are published on EAC intranet and send by email.
- **Customers and the public** are informed through public announcements and EAC website.



2. EAC Response to COVID-19

- Before implementing measures that affect personal data, the basic data protection principles must be considered.
- According to the European Data Protection Board (EDPB):

“Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. ... even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects...”



3. GDPR Compliance Obligations



3. GDPR Compliance Obligations

1. Legal Basis for the processing

Article 6(1) of the GDPR: All data must be processed lawfully, including data collected within the framework and policy adopted to fight the COVID-19 pandemic.

E.g. consent, performance of a contract, compliance with a legal obligation, to protect the vital interests, for the public interest, legitimate interests.

Article 9(2)(i) concerning the processing of special category data, including medical data and health data, *is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices...*



3. GDPR Compliance Obligations

2. Necessity

Articles 6 and 35 of the GDPR, the necessity of data processing for the protection of public health and public interest, should justify the processing and the intrusion in the data subjects' privacy when this occurs without consent.



3. GDPR Compliance Obligations

3. Proportionality

Article 35 Intervention to privacy and the processing of personal data must be **DIRECTLY** connected to the **PURPOSE** of Protecting Public health.

The principle of proportionality must be combined with **transparency** and **fairness** when deciding new measures, taking into consideration the context where a society is for now.



3. GDPR Compliance Obligations

4. Accurateness and continuous updates

There is an obligation to keep records accurate and updated. Information that is not needed anymore should be deleted/destroyed.



3. GDPR Compliance Obligations

5. Processing time

Personal data processing time must be the absolutely minimum necessary to succeed in protecting public health from COVID-19.



3. GDPR Compliance Obligations

6. Technical and Organisational Measures

A Data Controller must process personal data in a safe and consistent way, employing technical and organisational measures to reduce risk and to guarantee, to the extent possible, integrity of personal data, privacy and confidentiality principles.

Data Controllers must **PROVE** their compliance with all GDPR Principles, especially at these times.



3. GDPR Compliance Obligations

Data Subjects' Rights

Information on data processing purpose, the time of processing, their rights, at the time of providing consent
Information on what types of data the Processor processes.

Access, correction of personal data

The right to be forgotten

Transfer of personal data to third parties.

Withdrawing consent at any time.

COVID-19 is not a justification to abstain from satisfying Data Subjects' rights.



3. GDPR Compliance Obligations

EAC GDPR Procedures

Implementing a **Privacy Policy**

Maintaining an up-to-date **Data Processing Record** containing all processes including new ones implemented due to COVID-19.

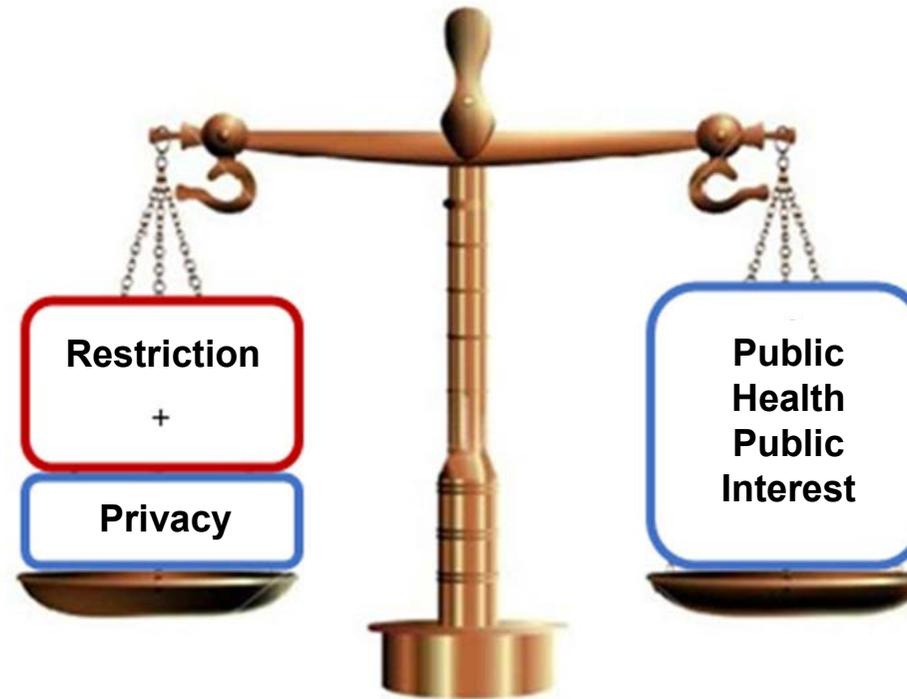
Implementing a Procedure to manage **Data Subjects Requests** and third-party requests.

All possible data breaches traced are reported to the Data Commissioners Office according to the **Managing of Data Breaches Procedure**.

Conduct **Data Protection Impact Assessments** before and during the processing of personal data, where needed.



3. GDPR Compliance Obligations



To justify measures that interfere with privacy, they must be proportionate to the purpose of processing, hence, the protection of public health.



4. Recommendations & Opportunities



4. Recommendations & Opportunities



1. Informing Data Subjects

Personnel, customers and all affected persons must be kept informed on GDPR/ COVID-19 Policies during the processing.

Information on the purpose, the way of processing and how EAC/Controller decided to implement the least invasive measures to help prevent COVID-19 contamination.

Where necessary, consent should be obtained where the Data Subject is properly informed.



4. Recommendations & Opportunities

2. Notifying the Data Processors

Where the measures will be implemented by Processors (e.g. security measuring temperature at entrance), Processors and their personnel must be informed and trained in GDPR issues and the Privacy Policy of the Data Controller.

A Data Processing Agreement must be in place and if needed it must be reviewed.



4. Recommendations & Opportunities

3. Teleworking

Employees working from home must follow special instructions (equipment, data).

In Cyprus we do not have a special law for teleworking.

Guidance stems from the European Commission Report on the Implementation of the European social partners' Framework Agreement on Telework (2.7.2008) under which employers need to respect their employee's privacy when using a laptop, the internet, the phone and other communication means and to keep them informed on all restrictions concerning private purposes.



4. Recommendations & Opportunities

4. Videocalls and recordings of meetings

The use of applications such as Skype for Business, Microsoft Teams, Zoom, Webex and Go to Meeting must be assessed concerning the security of transferred data.

Participants must be at liberty to activate and deactivate their microphone and camera.

When meetings are recorded (Board of Director meetings) a policy on recordings should be in place and processing of data (including mapping) must be in the Record of Processing Activities.



4. Recommendations & Opportunities

5. Performing DPIAs

Where the processing concerns a large scale of data subjects and special category data like health records, EAC/Controller needs to do a Data Protection Impact Assessment (DPIA).

Why? To assess the risk and decide to take extra measures.

At EAC we use a special form to do a DPIA and the responsible Manager may then ask for the opinion of the DPO.



4. Recommendations & Opportunities

6. Cooperation

**The COVID-19 Task Force
The Management
The GDPR Team & the DPO
The Head of Systems Security
To design and implement
policies and procedures to
avoid privacy breaches.**





Electricity
Authority
of Cyprus



Thank you for your attention!

*Pictures used are from <https://unsplash.com>, their use is free and does not breach intellectual property rights.