Data Protection in times of COVID-19
The death of privacy or a new challenge?

Prof. Lilian Mitrou

University of the Aegean

Institute for Privacy Law, Data Protection and Technology /EPLO

…the moment you realise the world has changed…

- Main data protection issues before the outbreak of Covid 19
  - How to face **AI challenges**? Do we need (a) new r(R)egulation?
  - **Assessment of application/ applicability of GDPR**
  - **Face Recognition Systems** – The "Clear View" Application
  - **Extensive use** of personal data for **security and law enforcement purposes**
  - Pending adoption of **e-Privacy Regulation**

…and then came COVID-19

- Some have even asked whether Covid-19 will (or should) set **an end to data protection**
- Some have emphasized the **implications** of the fight against corona virus **for the protection of the right to (informational) privacy** and other fundamental rights and freedoms
- Is the respect for fundamental freedoms **at odds with the efficient monitoring of spread of COVID-19**?

Data protection rules (such as the GDPR)

- …..**do not hinder measures** taken in the fight against the coronavirus pandemic
- The fight against communicable diseases is a **valuable goal** shared by all nations and therefore, should be supported in the best possible way…..(EDPB)

- Are **still applicable and binding**

- **even in these exceptional times**, data controllers (and processors) must **ensure the protection** of the personal data of the data subjects

The General Data Protection Regulation

- enables (Art. 6) the processing of personal data, for **reasons of public interest**- in particular when it falls under the legal mandate of the public authority provided by national legislation and the conditions enshrined in the GDPR
- foresees **derogations to the prohibition of processing** of certain special categories of personal data, such as health data
  - where it is necessary for **reasons of substantial public interest in the area of public health** (Art. 9.2.i)
  - **on the basis of Union or national law** where there is the need to protect the vital interests of the data subject (Art.9.2.c)
  - Where the processing of personal data may be **necessary for compliance with a legal obligation** to which the employer is subject such as **obligations relating to health and safety at the workplace** (Art. 9.2.b)

Requirements for the democratic emergency State

- The processing of personal data (health data, location data etc.) should be based on **clear, precise and accessible rules**
- The **necessity and proportionality of measures** with regard to the legitimate objectives pursued, i.e. to safeguard the public health objective, should be demonstrated
- **Specific purposes** should be defined setting the **context/ circle of controllers/ recipients and the extent of accessibility**
- The **transparency of the measures**, their scope and purposes must be preserved.
- The existence of an **independent oversight mec**hanism as well as the availability of effective remedies to the individual have to be ensured
- ….if it constitutes a necessary, appropriate and proportionate measure within a democratic society (**democracy test**)

Requirements for data controllers

- **Data minimization**: The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved.
  - Invasive measures, such as the "tracking" of individuals could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation).
- **Transparency and information duties**: data subjects should receive transparent information on the processing activities and their main features, including the retention period for collected data and the purposes of the processing
- **Compliance with "procedural/functional" obligations**
  - **Data Protection Impact Assessment (PROACTIVELY)**
  - **Adequate security measures and confidentiality policies**

Is COVID-19 a "game-changer"?

- A permanent shift or a temporary crisis management?
- Are measures here to stay after the crisis?
- Do we know the way back to (institutional) normality?

.

Restriction – not blanket suspension ad infinitum

The **European Data Protection Board** (June 2020) states

- Restrictions imposed **for a duration not precisely limited** in time and/or apply retroactively are **not compliant with the foreseeability criterion**
- Restrictions must be **strictly limited not only in scope but also in time**
- Restrictions adopted in the context of a state of emergency **suspending or postponing the application of data subject rights and the obligations** incumbent to data controllers and processors, without any clear limitation in time, would equate to a **de facto blanket suspension of those rights and would not be compatible with the essence of the fundamental rights and freedoms**

…some (pre)final thoughts … to avoid constitutional distancing

- COVID-19 **exceptional measures** should **not become the rule**
- "Even in these exceptional times, **the protection of personal data must be upheld in all emergency measures**, thus contributing to the respect of the overarching **values of democracy, rule of law and fundamental rights** on which the Union (*a democratic State*) is founded"
- Fundamental rights such as the right to data protection **can be restricted but not denied**
- **General, extensive or intrusive restrictions** that result in voiding a fundamental right of its basic content **cannot be justified**
- **Provisional and exceptional character to mitigate the risk of "constitutional distancing" or the "constitutional mithridatism".**

Thank you for listening

Prof. Lilian Mitrou (L.mitrou@aegean.gr)