

GDPR- the challenges of covid-19 in the hospitality sector

Athens, 18 June 2020

Nicolas Kanellopoulos
Lawyer
**Executive Director of the Institute for Privacy Law,
Data Protection and Technology of “European Public Law Organisation”-EPLO**

Covid-19- Challenges in the hospitality sector

A fair balance must be struck between the reopening of the economy and the “reset” in tourism with health protocols and privacy protection measures

- Hospitality sector urged to adopt **protocols** and **procedures** that ensure protection of customers and employees
- Privacy protection by design and by default
- Precautionary measures: they must not lead to stigma, disproportionate control or restriction of individuals
- Confidentiality of information and privacy on all confirmed or suspicious cases
- Collection of **no more data than necessary**
- Understand **why** personal data is collected and **for which purpose**
- **Special caution in terms of collecting and processing health related data**

Best practices in the adoption of health protocols

- Compliance and cooperation with public supervisory authorities (EODY)
- Efficient management of incidents
- Training of employees
- Cooperation between health service providers and hospitality sector
 - Involve all necessary stakeholders in the decision making
 - Ensure that agreements on data processing have been signed
 - Ensure that data subjects are properly informed on the processing
 - Transfer of data only where necessary on the proper legal basis



Application of art. 5 para 1 GDPR in the Covid-19 response plan

- Data shall be collected for specific and legitimate purposes (protection of public health)
 - Data shall be relevant, appropriate and shall be limited to the specific processing purpose
 - Data shall be accurate
 - Data should only be kept for as long as necessary in the context of the Covid-19 response plan
 - Security and confidentiality of data processing at all stages
- Where data processing may lead to high risk of data subjects' rights and freedoms, a **data privacy impact assessment** may be necessary

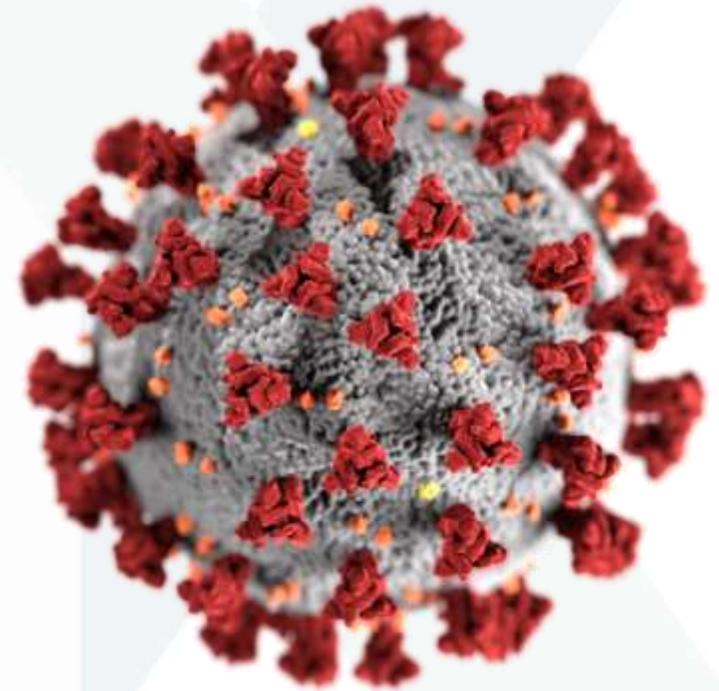
The use of new technologies in the fight against Covid-19

- The National Public Health Organization and the World Health Organization (WHO) remain vigilant regarding the evolution of the pandemic
- Data controllers must follow guidance issued by WHO, as well as by national supervisory authorities
- In EU, European Commission has issued guidance on the development of electronic applications in the fight against Covid-19
- Such applications could contribute to the early detection and protection of the spread of the pandemic
- The use of new technologies shall not lead to disproportionate restriction of data subjects' rights

The use of new technologies in the fight against Covid-19

In the context of strengthening the sense of safety when travelling around the world, the use of a “**Covid-19 passport**”, could be used, which would include the following information:

- Traveler’s health condition before the trip
- Covid-19 immunity (if applicable)
- Validity period



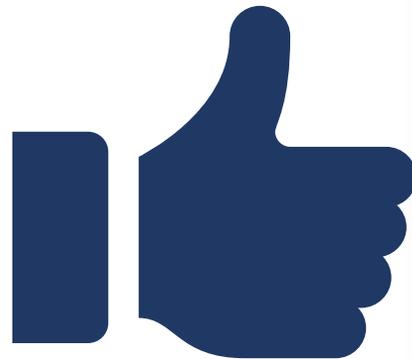
The use of new technologies in the fight against Covid-19

- The technical and legal provisions of such a procedure must be specifically set out worldwide to ensure the protection of transport and travelers
- In any case, the “Covid-19 Passport” should meet the standards of WHO, the competent supervisory bodies and the applicable Data Protection Legislation such as:
 - Data minimization principle
 - Storage limitation principle
 - Implementation of the appropriate technical and organizational measures

- High temperature as a possible indication for further testing
- **Temperature measurement** may raise privacy issues and may lead to an unauthorized disclosure of a person's physical condition
- Prohibition of access constitutes restriction of the freedom of movement of natural persons
- Guidance from the **Hellenic Data Protection Authority**. Temperature measurement shall be:
 - i. Temporary
 - ii. Not lead to identification of natural persons
 - iii. All data should be deleted immediately
 - iv. Not lead to systematic, continuous, generalized collection of personal data, no profiling and continuous renewal of employees' or customers' health profiles

The importance of a data protection plan

- All companies must revise and update their data privacy plans and policies
- Ensure that data subjects can exercise their rights
- Where new technologies are involved, a DPIA might be necessary
- The designation of a Data Protection Officer and a strong supporting team is of paramount importance



Thank you for your attention!

Nicolas Kanellopoulos
Lawyer
Executive Director of the Institute for Privacy Law,
Data Protection and Technology of “European Public Law Organisation”-EPLO

T. +30 210 3611 225, +30 210 3611 236,

F. +30 210 3610 227

Email: nicolas@kanell.gr

www.kanell.gr