SecureHealth Multiplier Event for
"Data Protection in Healthcare Sector."

Firstly, I would like to thank the organizers for inviting me to address this forum.

Health is the most important gift in life. It is what we wish to our friends, every time we share a moment. It should be the primary goal of every democratic society to ensure the wellbeing of its people, through an effective healthcare system.

However, the concept of the health sector is much broader than the concept of a healthcare system. It includes private health service providers, measures of monitoring a pandemic, pharmaceutical industries, researchers and industries developing new technologies. The list is not exhaustive.

So, where does the General Data Protection Regulation, in short the GDPR, come in?

According to the GDPR, health data, genetic data and biometric data belong to the special categories of personal data that should afford a higher level of protection. Therefore, organizations operating in the health sector which process health data, have a duty to apply a higher standard of protection to these data.

The protection of such sensitive data becomes more important especially when introducing innovative technological tools. In relation to this issue, I would like to underline that supervisory authorities welcome the use of new technologies in the health sector, as long as they can contribute to improving the quality of services provided, in the context of the GDPR.

I should also add, that the GDPR is a technologically neutral legal instrument. It does not prohibit or hamper the development of new

technologies. On the contrary, it is the role of the supervisory authorities to encourage and promote innovation, always in the frame of GDPR.

In the Preamble of the GDPR, it is explained that rapid technological developments and globalization have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

When introducing new technologies or when processing data for research purposes, the GDPR requires compliance with the principles set out in Article 5, of lawfulness, fairness, transparency, purpose limitation and data minimization. Also, it requires implementing appropriate technical and organizational measures, by default, at the stage of the design of the new technologies.

Furthermore, when new technologies are designed to process special categories of data, such processing should be in line with Article 9 of GDPR.

This Article allows the processing of special categories of data when, inter alia, the data subject has given explicit consent, when processing is necessary to protect the vital interests of a natural person, or it is necessary for preventive or occupational medicine, for assessing the working capacity of employees, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

Also, such processing can be conducted when it 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.

You may recall that during the pandemic a lot of new technologies where introduced and a lot of research was carried out. In 2020, the European Data Protection Board (EDPB) issued guidelines on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.

The EDPB notes that processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. Scientific research purposes should also include studies conducted in the public interest in the area of public health. Further, it is explained that determining necessary data which is needed depends on the purpose of the research even when the research has an explorative nature and should always comply with the purpose. It has to be noted that the data has to be anonymised, where it is possible and the proportionate storage periods shall be set.

In relation to new technologies, the EDPB is currently preparing guidelines on blockchain technology. It is a new technology with many prospective uses. As I mentioned during my speech in Parliament, several concerns are raised, particularly as regards the controller and the deletion of data. In other technological solutions, it is clear that it is the controller who is obliged to delete the data. But in blockchain solutions, there is a chain of intermediators and it is not always clear who is responsible for deleting data.

Research and new technologies are certainly an interesting topic for discussion. But my Office also deals with questions relating to day to day problems. One question that often comes up, is who can process health data and under what conditions.

According to the GDPR, data concerning health, genetic data and biometric data, may be processed by professional, subject to the obligation of professional secrecy under Union or Member State law. These data can also be processed by other persons also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Another question we are often asked, relates to the periods for retention of personal data. The GDPR provides that retention has to be proportional to the purpose of the processing.

According to the Opinion of our Office, dated 3rd of July, 2018, the retention period of health data must not exceed 15 years after the last registration by the controller in a filing system, or 15 years after the subject's death. These data may be stored for longer period only in a separate filing system and after appropriate technical and organizational measures will be implemented.

As regards processing in the context of scientific research or for statistical purposes as explained in the EDPB guidelines for the storage periods (timelines), criteria such as the length and the purpose of the research should be taken into account.

In my closing remarks, I wish to stress that every person or organization in the health sector is obliged to demonstrate compliance with the GDPR. The demonstration of compliance strengthens people's trust towards persons or organizations which process their personal data. Feeling safe and secure is a key element to our health and wellbeing.

I wish you a pleasant and fruitful discussion during the event.
Thank you for your attention.

Irene Loizidou Nicolaidou
Commissioner for Personal Data Protection

20/10/22