Covid-19 & GDPR
Challenges in Personal Health Data Generation

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

Covid-19 has changed our lives and the ways we socialize, work and interact with other people, both in the real and the digital world. During the pandemic, several measures had to be taken, which involved processing personal data. Vast amounts of information were generated, collected and stored. Scrutinizing these measures was a serious challenge for my Office.

The scrutiny was a two- step procedure. The first step was to check the lawfulness, the necessity and the proportionality of the measures and the technical and organizational safeguards put in place, in line with the General Data Protection Regulation - the GDPR. The second step was to ensure the balancing of public interest, against individual rights, as the GDPR demands.

At the same time, the pandemic posed an unprecedented challenge for health care systems, all over the world. In such difficult times, health care systems are vulnerable to fraud and to abuses of personal data. One has to remember that, according to the GDPR, health data deserve a higher level of protection and their processing should be subject to appropriate safeguards.

The Ministry of Health and the Deputy Ministry of Research, Innovation and Digital Policy, were also challenged by the pandemic. They were tasked to launch numerous technological tools, such as new platforms, databases and applications. All these tools generated vast volumes of personal data and had to be consulted with my Office, in a very tight time frame, before implementation.

My speech will focus on three topics. First, I will outline some of the measures taken during the pandemic and explain how my Office

was involved in their authorization, in the frame of mandatory consultations. Second, I will describe some safeguards put in place, for preventing abuses and fraudulent claims in the General Health System - the GHS. Finally, I will give some examples of complaints submitted to my Office, for alleged unlawful access to medical records in the GHS.

Starting with the first topic, it should be reminded that according to the GDPR, when a new technological measure, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment should be carried out and the measure should be consulted with the supervisory authority. This procedure ensures that potential risks have been identified and that safeguards have been put in place for mitigating those risks. In the context of these consultations, my Office was tasked to scrutinize all measures taken during the pandemic.

One of the first measures implemented, was the SMS Authorization. During quarantines, persons were permitted to exit their houses only for specific purposes and for a limited time. People had to send a request via SMS and receive an automatic reply for authorization. SMSs were sent to, and received from the person's telecommunications service provider. The provider retained the messages for 72 hours after their receipt. When this measure was waived, we sent letters to providers and confirmed that all the SMSs were automatically deleted after 72 hours.

Another measure was the Cyprus Flight Pass. It was a platform developed for ensuring that all passengers flying to Cyprus had the required health certificates. Requirements differed for countries of departure classified as high, medium and low risk. Inbound passengers, to issue their passes, had to enter their personal information, flight details and details of the health certificate they held. My Office ensured that access to these data was given only to competent authorities, according with the relevant Decrees of the Ministry of Health.

Also, we examined two data protection contracts. One for the processor/ contractor that developed the Cyprus Flight Pass and one for the labs that performed covid tests to inbound passengers. In addition, upon our instructions, an agreement was signed between the joint controllers (the Ministry of Health and the Ministry of Transport, Communications and Works) specifying their respective responsibilities, in relation to this platform.

Remote Education: Following various concerns that were expressed by students, parents, teachers and other organizations regarding the implementation of remote education, my Office conducted a series of on-site inspections at schools. Based on our findings, we instructed the Ministry of Education and Culture to:

a) prepare policies for implementing uniform practices for remote education,
b) provide information to students and teachers regarding the processing of their personal data,
c) provide information to all users about the secure usage of the platform and
d) prepare and submit to my Office a Data Protection Impact Assessment.

In addition, and following our recommendation, a Law was adopted to regulate remote education in primary and secondary schools. For higher education institutions, we issued an Opinion for monitoring on-line/ remote exams.

European Digital Covid Certificate (EUDCC): The EUDCC platform was developed to implement the EU Digital COVID Certificate Regulation. This Regulation was adopted to facilitate people's free movement across Member States. My Office ensured that the national technical solution complied with the EUDCC Regulation and the GDPR. Several safeguards were embedded for ensuring the availability and accuracy of the data.

When the Government decided to use EUDCC as national "safe pass", we expressed the opinion that this could not rely on the European Regulation and that it required a separate legal basis. Consequently, the Council of Ministers drafted a relevant Decision, which was consulted with my Office, before its adoption.

The COVSCAN Application: This app was developed for validating the authenticity of EUDCC Certificates, using QR Codes. Relevant Decrees of the Ministry of Health, defined who was authorized to use this app. My Office ensured that only necessary data (name and date of birth) were presented on the scanning device, when scanning an EUDCC and that no data were stored.

The CovTracer was used on a voluntary basis, for keeping track of users' movements in the last fourteen days, to help them remember with whom they may have come in contact. This application was replaced by the CovTracer-EN (Exposure Notification) application, which was also voluntary. Users could voluntarily indicate being covid positive, without revealing their identity. With the use of Bluetooth technology, other users got a warning if they came in close proximity to the device of the covid positive user.

The Ministry of Health has recently informed us that this app was terminated, disengaged from the European Portal and that steps were taken to be removed from App Stores.

One of the most important measures taken, was the Vaccination Portal: It allowed GHS beneficiaries to schedule appointments for vaccination. When vaccinated, the beneficiary' GHS medical record was updated with information such as the date of vaccination and the type of the vaccine that was administered. My Office was involved in its design, as of day one and provided guidance for its development and architectural structure. We ensured that in the envisaged portal, appropriate technical and organizational measures were embedded, for safeguarding the integrity, confidentiality and accuracy of the personal data.

During the pandemic, my Office received a lot of questions regarding the procedures for checking employees' certificates at the workplace. Employers' and employees' obligations, varied, according to the Decree in effect, at the time. We issued numerous press releases, for ensuring that no unnecessary data was generated and that only necessary information was collected and stored.

When my Office scrutinized all these measures, our primary goal was to ensure that all the measures were proportional to the epidemiological condition, at the time and that, there was a balance between public interest and individual rights. Looking back at those measures, two overarching conclusions can be drawn. First, technology did contribute to the fight against the pandemic. Second, my Office was kept quite busy during the pandemic.

The second topic I wish to address, concerns abuses and fraudulent claims in the GHS. When the Health Insurance Organization – the HIO, identified the risk of claims without offering any health services, a two- fold safeguard was consulted with and approved by my Office. When a doctor or a pharmacist submits a claim, the beneficiary receives a notification by email. A beneficiary, who did not receive a claimed treatment or did not get a claimed prescription, can report the case to the HIO for investigation. Also, in case of a doubt, a beneficiary can check his personal account, where more detailed information is provided.

While this procedure proved quite useful, it has some loopholes. Some beneficiaries do not check their emails frequently, and when they do, they do not remember if the claim is accurate. Also, many beneficiaries did not activate their account, for receiving more detailed information about the claims. Recently, the HIO asked my Office if these problems could be tackled, by providing more detailed information, in the emails sent to beneficiaries. Having

assessed the situation, we replied that, sending detailed health data by emails, entails serious risks. Instead, we suggested that each email includes a link to the beneficiary's account. This way, the beneficiary would be prompt and encouraged to activate it.

In another case, we examined HIO's demand that some Specialists submit photographs of their patients, to support their claims. The aim was to prevent fraudulent claims, by ensuring that a claim related to treating a pathological condition, which could be covered by HIO, and that it was not for cosmetic purposes. The Specialists, argued that, in some cases this was degrading for the beneficiaries, in particular when they had conditions in their genital area. Through their Association, they requested my Office's intervention. After discussing the issue with the HIO, a two- ply procedure was adopted. First, claims have to be supported by test results that justify the need for treatment. Second, if supporting photographs are also needed, they should be taken in way to respect the beneficiaries' dignity.

During the pandemic, concerns for fraudulent claims were also voiced for the offering of free rapid tests. At the beginning of the pandemic, the Ministry of Health employed a number of laboratories, to carry out these tests for free. A person who took the test, received the result by SMS. Often, due to human error, the message was sent to a wrong telephone number. If you received such a message, without having taken a test, you could reasonably assume one of two things. Either there was a typing error or the lab attempts to get paid for a test not done. Also, if the initials of the name, in the message, happened to match yours, you could reasonably wonder, how a lab you had never visited, got your name and telephone number. At the time, my Office received a number of complaints and we investigated them in collaboration with the Ministry of Health. All investigated cases, were attributed to human error and coincidence.

The third topic I wish to address, relates to alleged unlawful access to GHS beneficiaries' medical records. It has to be explained that each beneficiary is assigned to a Personal Doctor. When a beneficiary needs to be referred to a Specialist, the Personal Doctor will issue a referral. The beneficiary can choose and visit a Specialist, as long the referral is active. During the visit and for some time after, while the referral is still active, the Specialist can access the beneficiary's medical record.

A Specialist can also access a GHS beneficiary's medical record, without a referral, under two conditions. The Specialist is obliged to indicate in the GHS, which condition applies. The first condition is when a beneficiary visits the Specialist for a second opinion. In this case, the Specialist has to indicate that the beneficiary's consent was obtained, before access to the medical record. The second condition applies when a beneficiary is not capable to consent, for example because of being unconscious. When a Specialist has access to a medical record, the beneficiary receives a notification and can check the date, time and the reason for access.

My Office received a number of complaints relating to unlawful access to medical records, by unauthorized Specialists. In two cases, Specialists were fined by the Health Insurance Organization and my Office initiated administrative procedures against them. Because these cases are still under investigation, I am not at liberty of disclosing more details.

In my closing remarks, I wish to say, that when the HIO identifies a threat or a problem, it has to take steps for fixing or preventing it. These steps may include, upgrading the GHS or putting in place appropriate technical and organisational safeguards. When these steps involve processing beneficiaries' personal data, they have to be consulted with my Office. Problems arise, almost every day. We have an open line with the HIO for solving them.

I wish to recite a text from the GDPR, which in my opinion reflects the essence of this legislation: "*The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.*"

Thank you for your attention.