REDA Conference
May 2023

First, I would like to thank the organizers for inviting me to address the Regulation and Enforcement in the Digital Age Conference, for the third consecutive year. Conferences like REDA give to experts and specialists from various fields, the opportunity to be informed on developments in their field, but also to exchange views on matters of common interest and concerns.

One of the topics that will be discussed during this year's REDA, is Artificial Intelligence. In 2021, the European Commission presented a Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts. This proposal aims at improving the functioning of the internal market, through a uniform legal framework, in particular for the development, marketing and use of AI, in conformity with Union values.

The European Data Protection Board (the EDPB) and the European Data Protection Supervisor (the EDPS) issued a Joint Opinion for the AI Act. While we welcome the proposal, we raise a number of concerns, in particular as regards the scope of the Proposal which excludes the use of AI in the frame of international law enforcement cooperation and as regards "social scoring". Social scoring refers to profiling individuals, based on certain behaviours and categorizing them as high, medium or low risk, for rewarding or penalizing them, accordingly. The EDPB and the EDPS believe that social scoring could lead to discriminations and that it should be prohibited under all circumstances.

AI has many uses and it could have a positive impact on our lives, when used responsibly. At the same time, it poses many risks. In a recent report issued by the European Parliament on March 23rd, it is noted, and I quote, that "*New AI tools in general offer massive potential for developments in industry, agriculture, health, education and other areas. However, many scientists and politicians are calling for the establishment of a legal and ethical framework to avoid potentially determinant impacts from the use of such technologies*".

One of the main concerns of the Data Protection Authorities, is the quality of algorithms used in AI. The EDPB, during its April Plenary discussed the measures taken by the Italian Data Protection Authority, the Garante, against Open AI, for its ChatGPT service. The EDPB decided to set up a taskforce for fostering cooperation and for facilitating the exchange of information among

the Authorities and for deciding on the way forward. In this context, the EDPB has started a dialogue with Open AI. My Office participates in this taskforce.

AI is also linked to the topic of Smart Cities, that will be discussed later on. My Office is in the process of prior consultation with a Municipal Authority, that wishes to deploy smart cameras for monitoring traffic in certain roads and people's movement in the city centre. These cameras use AI to detect the display of malignant or deviant behaviour, such as the intention to vandalize city property or to spray graffiti on monuments. Data Protection Authorities welcome such initiatives. But at the same time, they raise caution, with respect to the right to privacy.

In 2001, the Dutch Data Protection Authority imposed to the municipality of Enschede a fine of 600,000 euros, for using Wi-Fi tracking in the city centre in a way that is prohibited. The Wi-Fi tracking made it possible to track shoppers and people who live or work in the city centre. Sensor equipment was placed in the shopping streets that detected the Wi-Fi signals from the mobile phones of passers-by. This makes it possible to measure how crowded the street is by counting how many phones are near a sensor at a particular time. If, however, you monitor over a longer period of time which phone passes close to which sensor, that 'counting' becomes tracking.

Last week, the EDPB, after public consultation, adopted its Guidelines on the use of facial recognition technology in the area of law enforcement. While it acknowledges that smart cameras, are not directly linked to facial recognition, the EDPB notes that digital techniques for detecting abnormal behaviours or violent events, and for recognizing facial emotions or even silhouettes, are still subject to personal data protection rules. This type of detection system may be used in conjunction with other systems aiming at identifying a person and thereby being considered as a facial recognition technology.

Another topic that will be discussed later on, is the use of spyware and the interception of communications. Several articles have been published about the use of PEGASUS and PREDATOR in Greece and in other EU Member States. Some articles report companies based in Cyprus being involved in providing these spywares to EU and third countries' governments. In November 2022, PEGA, the European Parliament Committee mandated to investigate the use of such spyware, visited Cyprus and issued a draft Report after hearing several Officials, NGOs, reporters and concerned citizens. My Office closely follows this issue and in collaboration with the Greek Supervisory Authority.

At this point I should say few words about the Digital Services Act (DSA) which will be discussed later on. The DSA, along with the Digital Markets Act (DMA) and the Data Governance Act (DGA) are part of a package of

legislative EU Acts for the digitalization of the internal market. They aim at creating a safer digital space where the fundamental rights of users and consumers are protected and at establishing a level playing field for businesses. To this day my Office has not been consulted with on any national legislative proposals, for the implementation of these Acts.

Last but not least, I wish to touch the issue of cybersecurity. The recent attacks to the University of Cyprus, the Open University and the Department of Land Registry, have shown that we should never put ourselves at ease and that we need to remain vigilant at all times. Due to the fact that there is an ongoing investigation, I am not at liberty to openly discuss this issue. But I should mention that my Office is in close cooperation with the Digital Security Authority and that we have formally informed the EDPB about these attacks.

Hacking attacks such as these, raise questions of liability and compensation to affected individuals whose personal data had been leaked in the dark web. On 27 of April 2023, the Advocate General issued an Opinion for CJEU's Case C-340/21, in relation to the hacking of the Bulgarian Tax Authority's information system. As a result, information regarding millions of persons had been leaked on the internet. An affected person filed a Court case for compensation and the Bulgarian Court referred a number of GDPR questions to the CJEU, regarding the conditions for awarding compensation for non-material damage.

The Advocate General concluded that unlawful access to personal data by third parties leads to liability for presumed fault on the part of the controller and gives rise to nonmaterial damage for which compensation can be awarded. In order to be exempt from liability, a controller must demonstrate that it is not in any way responsible for the event giving rise to the damage. Fear of possible misuse of the data in the future can constitute non-material damage which can justify compensation only if it is actual and not simply trouble or inconvenience.

Thank you for your attention. I am confident you will have a fruitful and constructive Conference.