Human Rights Council Resolution 42/15 on the right to

privacy in the digital age

* Response by the Republic of Croatia -

Advances in technology and the ability to analyze large amounts of data, artificial intelligence, and machine learning have facilitated the creation of profiles and automated decision-making that can significantly affect the rights and freedoms of individuals. The wide availability of personal data on the Internet and the ability to find correlations and make links make it possible to identify, analyze and predict aspects of the personality or behavior of individuals and their interests and habits.

Having this in mind, Ministry of Economy and Sustainable Development of the Republic of Croatia started drafting the National Plan for the Development of Artificial Intelligence for the period 2021-2025. The Working group for the development of this document has been appointed gathering experts from academia, business sector, civil society and the public sector. The draft of National Plan will be updated in line with the new EU vision published in Commission’s AI package in 2021 proposing new rules and actions.

Since the National Plan is still in drafting phase, the main priorities are yet to be defined. In terms of technologies/applications, main priorities of the draft of National Plan are the following:

• emphasize technological development as the foundation of economic growth and encourage the acceptance of artificial intelligence in the public and private sector;

• adequately prepare for the socio-economic changes of AI implementation in society;

• provide an appropriate ethical and legal framework for the usage of artificial intelligence systems;

• propose measures to enhance research and cooperation between the private and public sectors, and increase investments in development and application of artificial intelligence systems;

• increase the application and acceptance of artificial intelligence systems by creating opportunities for testing and experimentation in the thematic priority areas of the Smart Specialization Strategy (S3);

• accelerate the adoption of artificial intelligence systems in the public sector by supporting public procurement systems based on artificial intelligence and helping to transform public procurement procedures themselves.

In terms of legislation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) is fully binding and directly applicable in the Republic of Croatia since 25th May 2018, and its provisions must be complied with by all entities that process personal data of natural persons in the European Union as part of their activities, and in certain cases also entities outside the European Union.

General Data Protection Regulation provides for specifications or restrictions of its rules by the law of a Member State, and Member States may, to the extent necessary for harmonization and to make national provisions comprehensible to the persons to whom they apply, incorporate elements of the Regulation into their national law. Consequently, the Republic of Croatia adopted the Act on the Implementation of the General Data Protection Regulation, which was published in the Official Gazette (OG 42/18).

General Data Protection Regulation introduces new provisions to eliminate the risks arising from the creation of profiles and automated decision-making, which primarily, but not exclusively, relate to privacy.

General Data Protection Regulation applies to the processing of personal data that is fully automated and to the non-automated processing of personal data that form part of a storage system or are intended to be part of a storage system. In order to prevent the creation of a serious risk of circumvention, the protection of individuals should be technology neutral and should not depend on the technologies used.

The definition of "processing" under the General Data Protection Regulation means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Definition of "profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

It is primarily important to point out that any collection and processing of personal data in accordance with the General Data Protection Regulation requires the existence of a legal basis under Article 6 of the General Data Protection Regulation which stipulates that processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

If the legal basis for the processing of personal data is the legal obligation of the controller, then that legal basis must be laid down in Union law or the law of the Member State to which the controller is subject, and that legal basis must specify the purpose of the processing.

If it is a matter of processing special categories of personal data, then in addition to the legal basis referred to in Article 6 of the General Data Protection Regulation, there must be exceptions to the general prohibition on processing special categories of personal data referred to in Article 9 of the General Data Protection Regulation.

Within the principle of transparency, it is important to point out that in accordance with the General Data Protection Regulation, in addition to the other information referred to in Article 13, the controller shall, at the time when personal data are obtained, provide the data subject with  information on the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Pursuant to Article 21 of the General Data Protection Regulation, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions.  The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Furthermore, Article 22 of the General Data Protection Regulation stipulates that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. However, paragraph 1 of Article 22 of the General Data Protection Regulation shall not apply if the decision is:

1. necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

Pursuant to Article 35 of the General Data Protection Regulation, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

The data protection impact assessment referred to in paragraph 1 shall be mandatory in particular in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

The Act on the Implementation of the General Data Protection Regulation (OG 42/18) stipulates the processing of biometric data in a way that public authorities may process biometric data only if laid down by law and necessary to protect persons, property, classified data or professional secrets, taking into consideration that interests of data subjects which are contrary to the processing of biometric data should not prevail. It shall be considered that the processing of biometric data is in accordance with the law if it is necessary to fulfil obligations from international treaties with regard to identification of individuals crossing the state border.

Furthermore, processing of biometric data in the private sector may be carried out only if laid down by law or necessary to protect persons, property, classified data, professional secrets or for individual and reliable identification of users of services, taking into consideration that interests of data subjects which are contrary to the processing of biometric data from this Article should not prevail. The expressly stated consent of such data subjects given in accordance with the General Data Protection Regulation shall represent the legal basis for processing of biometric data of data subjects for the purpose of reliable identification of users of services.

Processing of biometric data of employees for the purpose of recording working hours and entry and exit from official premises shall be allowed, if laid down by law or if such processing is carried out as an alternative to another solution for recording working hours or entry and exit from official premises, under the condition that the employee has given an explicit consent for such processing of biometric data in accordance with the General Data Protection Regulation.

The provisions of this Act on processing of biometric data shall apply to data subjects in the Republic of Croatia if the processing is carried out by:

– a controller established in the Republic of Croatia or providing services in the Republic of Croatia

– a public authority.

The provisions of this Act on processing of biometric data shall not affect the obligation to carry out impact assessment in accordance with Article 35 of the General Data Protection Regulation.

The provisions of this Act on processing of biometric data shall not apply to the area of defence, national security and the security and intelligence system.

It is important to point out the Electronic Communications Act (OG 73/08, 90/11, 133/12, 80/13, 71/14 and 72/17), which regulates the field of electronic communications, namely the use of electronic communications networks and the provision of electronic communications services, provision of universal services and protection of the rights of service users, construction, installation, maintenance and use of electronic communications infrastructure and related equipment, conditions of competition and rights and obligations of participants in the market of electronic communications networks and services, effective radio spectrum management and address and numerical space, digital radio and television, data protection, security and integrity of electronic communications networks and services and inspection and control in electronic communications, as well as the establishment of a national regulatory body for electronic communications, postal services and rail services, its structure, scope and competencies and decision-making and dispute resolution in electronic communications.

In conclusion, while taking into account the mentioned national legislation, we emphasize the need to monitor the constant development of technology and experience while takling the challenges it brings in order to monitor and act in a timely manner within data protection field and to meet the best possible challenges and opportunities for individuals and society, and the ways in which risks can be countered and opportunities enabled through law and technology.