**Artificial intelligence, including profiling, automated decision-making and machine-learning technologies (hereinafter referred to in short as AI) in Hungary**

1. **Legislative and regulatory framework**

Hungary, as a Member State of the European Union has to apply the provisions of the General Data Protection Regulation[[1]](#footnote-1) (hereafter: GDPR) since it became applicable on 25 May 2018. The GDPR has introduced some general regulation on automated decision making in the context of personal data processing in Article 22. The provisions of this Article are only applicable if the data processing is solely based on the automated means and the decision made by the machine has legal effects concerning the data subject or similarly significantly affects him or her. This provision constitutes a general prohibition on decision-making based exclusively on automated data processing. The regulation includes profiling based on such a decision-making process.

There are, however, exemptions from this general prohibition set forth in Article 22(2). Accordingly, the prohibition cannot be applied if the decision is:

1. necessary for entering into or performing a contract between the data subject and the data controller;
2. *authorised by European Union or Member State law,* to which the datacontroller is subject and which also lays down suitable measures to safeguard the data subject’ rights and freedoms and legitimate interests; or
3. based on the data subject’s explicit *consent.*

The Hungarian legislator introduced some legislative measures that allow for certain data controllers to carry out automated decision-making (and profiling) in certain situations. Note that most of the following examples from Hungarian law had already been introduced before the applicability of the GDPR, 25 May 2018.

**Example No. 1:** Act CL of 2016 on the Code of General Administrative Procedure

The Hungarian Code of General Administrative Procedureregulates general applicability of automated decision making as follows:

*“Section 40 [Automatic decision-making]*

*Automatic decision-making shall apply if*

1. *it is permitted by an Act or government decree,*
2. *all data are available to the authority at the time of the submission of the application,*
3. *decision-making does not require deliberation, and*
4. *there is no party with opposing interests.*

Moreover, Section 42 of the same Code provides for the right to request the authority to reconsider the automatic decision in a full (human-controlled) procedure as follows:

“*Section 42 [Adjudicating an application in a full procedure]*

*If no appeal lies against a decision made in an automatic decision-making procedure […], the party may request the authority, within five days following the communication of the decision, to reconsider his application in a full procedure.*”

Finally, Section 80 (2) a) contains the following administrative safeguard regarding automatic decision-making:

„*Where the authority refrains from adopting a final decision within the administrative time limit (legitimate silence), the party shall be entitled to exercise the right applied for. Legitimate silence shall be allowed if it is not excluded by an Act or government decree in a case which may be administered through automatic decision-making.*”

**Example No. 2.**: Act CXXV of 1995 on national security services

The Hungarian Act on national security services regulates automated decision making in relation to the Passenger Names Record (PNR) System. In Hungary, the PNR System is used to share data of air passengers between airline companies and a specialised national security agency, the Counter-terrorism Information and Criminal Analysis Centre for counter-terrorism and crime prevention purposes. The establishment of the national PNR system is based on European law.

The relevant provisions of the Act reads as follows:

Section 52/H. (6): *“The Counter Terrorism-information and Criminal Analysis Centre carries out its risk-assessment activity at first by way of automated risk assessment. If the automated risk assessment results in a hit, the Counter Terrorism-information and Criminal Analysis Centre investigates the hit individually by human intervention.”*

**Example no. 3.**: Act LIII of 2017 on the prevention of money-laundering and terrorism financing.

The Hungarian Act on the prevention of money-laundering and terrorism financing regulates automated decision making in relation to the national Financial Information Unit (hereinafter “the FIU”). The FIU’s task is to analyse financial and transaction information sent by financial institutions for anti-money-laundering and anti-terrorism financing purposes. The establishment of the national FIU is based on European law.

The relevant provisions of the Act reads as follows:

Section 39. a): *“[…] The FIU during its operative analysis compares the received data with the data stored for analysis and evaluation purposes taking into account the risks specified in the national risk assessment methodology. The risks assessment is automated.”*

**Example no. 4.**: Act CLXXXVIII. of 2015 on registration and computing system on face analysis

The Hungarian Act on registration and computing system on face enables the Hungarian Police to use an automated compare system in order to check somebody’s identity. The procedure is as follows: if there is someone who is not able or does not want to prove his/her identity to the police, the officer takes a picture of the person with a specialized device, than sends the picture on the spot to the face analysis center. The face analysis center responds approximately in one or two minutes after comparing the picture with the listed ones in the registration, and sends back five pictures that are the most similar to the one taken by the officer. Then it is the officer’s task to choose one of the five, that – according to his/her opinion – shows the person of whom identity he/she wants to know, and the personal data attached to the chosen picture will be sent over. According to the Act the officer can use the face analysis system as well if the person identifies himself but there is doubt about the genuinity of the identification.

**II.** **AI in Hungary in relation to addressing the COVID-19 pandemic: Applications in the context of fighting the COVID pandemic**

**Example No. 1: The Home Quarantine System (hereinafter referred to as HQS)**

The Home Quarantine System (HQS; https://hazikaranten.hu/) is a smartphone application that allows the competent authority to check compliance with quarantine rules for persons placed in official home quarantine, instead of physical police presence in accordance with the Hungarian Government’s 181/2020. (V.4.) government decree. The app is intended to be a tool for authorities and home quarantined individuals, so its use is voluntary. The person in the official home quarantine may decide to download and use the HQS application and verify the compliance with the home quarantine rules by performing remote check-ins available through the application or refrain from using the application and thus choose the daily personal police checks.

A quick rundown on how the system works:

The user downloads the application to his/her smartphone, registers, and then performs a remote check-in from the home quarantine with a selfie photo while the system automatically retrieves the GPS data of the device. Based on the photo, the system verifies the identity and compares the GPS data with the home quarantine address data. Remote check-in requests are sent to the HQS user at random time intervals between 8.00AM and 8.00PM via SMS. The process is automatic, human operators are involved only in case of registration- or remote access incidents. HQS only reads the GPS data of the smartphone during remote check-ins, it cannot be used for continuous tracking of the user. After 60 days from the end of the official home quarantine period (in accordance with the relevant legislation), the user is automatically deleted from the database, or if the user does not wish to continue using the application during home quarantine, he can notify the Hungarian Police to erase them from the HQS. In the latter case the user will be deleted manually from the database and will continue to be personally monitored by the police.

The system also sends a health assessment questionnaire to the user three times a day, which is completed on a voluntary basis. The completed questionnaire is automatically uploaded to the Hungarian Electronic Health Service Repository, where the data can be accessed by the person's GP. The system also evaluates the questionnaire anonymously according to a pre-defined set of criteria.

The purposes of HQS:

1. Taking epidemiological measures and the prevention of the violation of quarantine orders, tracing the person under quarantine using location data, verifying the location of the smartphone of the data subject, alarm in case of abandonment of the quarantine.
2. Facilitating treatment and taking epidemiological measures (analysis of medical history in order of treatment, health monitoring).

The HQS application was developed and offered by the Asura Technologies Ltd. The HQS system runs on the servers of “NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.”, which is 100% owned by the Ministry of the Interior. Data transmissions associated with the system are always encrypted.

Users must always fill in a declaration regarding the use of HQS before registration; they must also give their consent to a declaration of use in order to access the app within the application. If the users prefer to use the health questionnaire function, they must give their explicit consent during registration.

The HQS system does not store medical data, only acts as an intermediary for the Electronic Health Service Repository, where medical data are stored.

The role of operator is performed by Hungarian Police staff. Technical support for the registration and remote check-in process is provided by a “chat support” anonymously for the user, meaning that users are not asked for any personal or other piece of information based on which they could be uniquely identified.

**Example No. 2: Contact tracing app (hereinafter referred to as VirusRadar)**

The Ministry for Innovation and Technology (MIT) announced the so called “VirusRadar”, a contact tracing app on 14 May 2020.

To use the app, a registration is required. For the registration, the data subject only needs to enter his / her mobile phone number, then the identification code will be sent via SMS.

The purposes of VirusRadar:

1. To map the spread of the infection, to protect health, and to reduce the spread of the epidemic by participating of the people in the fight against Covid-19 infection.
2. The contact tracking activities of the National Centre for Public Health (as data controller according to their Privacy Notice published on their website: https://virusradar.hu/privacy-policy) are supported by the application, which provides a more accurate picture of the risky contacts’ data from the last 14 days.

For aim 1, the app collects and stores for 14 days:

* the AppID,
* the detection date and the AppID of the other device,
* the time spent in close contact,
* the distance between the two devices.

For aim 2, the app transmits the following data exclusively to the data controller:

* the fact of the infection,
* the mobile phone number,
* the AppID,
* the data of the last 14 days:
	+ - the detection date and the AppID of the other device,
		- the time (more than 20 min) spent in close contact,
		- the distance (less than 2 m) between the two devices

The Governmental IT Development Agency (as data processor) stores the voluntarily transmitted and encrypted personal data on its server for 30 days. The application is developed and operated by the data processor.

According to their Privacy Notice the data controller can access only to the data processed on the server for the aim of taking necessary measures in order to the public health and epidemiology interest, referring to the section 4 d) of the Act 47 of 1997 on the health data processing, and under the legal basis of art. 6 (1c) and the aim of art. 9 (2i) of the GDPR.

1. 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) [↑](#footnote-ref-1)