OPEN LETTER

TO:

- Romanian Ministry of Internal Affairs
- Romanian National Supervisory Authority for Personal Data Processing
- Romanian People’s Advocate
- Romanian Chamber of Deputies - Commission for the investigation of abuses, corruption and petitions

The signatory parties represent organizations of fundamental rights, and representatives of the community of specialists in the field of data protection on the territory of Romania. Through this open letter we express our concern regarding the observance of the fundamental principles regarding the privacy by implementing the facial recognition system which is to be acquired by the General Inspectorate of the Romanian Police through the acquisition procedure with the number CN1014432¹, while formulating several requests publicly.

We draw attention to the obligation of public authorities to respect and protect the intimate, family and private life, pursuant to Article 26 (1) of the Constitution of Romania, art. 151 of the TFEU, art. 8 of the COE and art. 71 of the New Civil Code - The right to privacy.

We emphasize that the signatory organizations do not stand against the implementation of new technologies meant to bring more security to the inhabitants of Romania, supporting instead a responsible approach, respecting the right to privacy according to the applicable national and European legislation.

We consider that the decision to implement a mass monitoring system, which targets all the inhabitants of Romania, should have been taken, according to the legal requirements, following a real and transparent risk assessment process, involving both the National Supervisory Authority as well as representatives of civil society. The lack of this process determines us to look with skepticism both the legality of the implementation of this system and the ability to fulfill its purpose without prejudice to the rights of all citizens of Romania.

The drafting of the Tender Specification disregarding the obligations for the establishment of adequate guarantees for the rights and freedoms of the persons will result in the acquisition of a facial recognition system that cannot be used under legal conditions. The General Inspectorate of the Romanian Police, under the subordination of the Ministry of Internal Affairs, should have conducted an impact analysis before starting any action related to the processing of personal data, such as the purchase of the software application, and to include fundamental criteria to ensure compliance with the principles. “Privacy by design” and “privacy by default”.

¹ http://sicap-prod.e-licitatie.ro/pub/notices/c-notice/v2/view/100069755?fbclid=IwAR2R8so4QmYTLdhr1Abh2FIE0Oecunc04_rbKtdSaF_gaPFReNbijHHYX4
All the signatory organizations support the introduction of a new technology regarding the **increase of the degree of combating and elucidation of the crimes**, which respects the right to privacy of the persons, as well as other obligations stipulated in law. We emphasize that the interoperability of personal data must be based on transparency and observance of the principles of personal data collection, so that citizens can be confident that their data are processed properly, without the risk of an imbalance.

Therefore, we ask you to make sure that you followed all the steps that are required to enable the system to be operational, its effectiveness to be optimal, in accordance with the legal provisions, without prejudice to the rights and freedoms of individuals. We ask you to consider our following proposals in order to obtain the conformity of the technical solution regarding the implementation of the facial recognition system.

**The premise**

Following the publication of a press release\(^2\) at the beginning of this year, on the 27.08.2019 was published in **Electronic Public Acquisition System of Romania (SEAP)** the notice of participation with the number CN1014432 regarding the acquisition of **an IT solution for facial recognition + training** in within the framework of the project "Development of the facial identification and recognition system (NBIS) and its interconnection with the law enforcement authorities in the EU through sTESTA", the contracting authority being **the General Inspectorate of the Romanian Police**, subordinated to the Ministry of Internal Affairs.

The use of facial recognition systems has been the subject of much controversy worldwide, which is why the acquisition of such technology has immediately attracted the attention of organizations in Romania dedicated to the protection of the rights and freedoms of individuals.

For the introduction of such a technology, we consider dialogue to be essential and the consultation with the interesting parts, prior to issuing the Specifications for the acquisition of the facial recognition system so that the drafting of the purchase requirements meet the criteria for respecting privacy.

As this dialogue did not take place, we come proactively in support of the Contracting Authority by analyzing the documentation of this procurement and we found:

- the lack of fulfilment of the technical requirements, regarding the security of the data processing, obligatory for functioning in the conditions of the law of such a system.
- the lack of transparency regarding the implementation of the system in accordance with the principles regarding the privacy compliance
- the lack of information regarding the security measures implemented for the use of the technical solution
- the lack of information regarding the exercise of the rights of the data subjects

---

\(^2\) [https://www.politiaromana.ro/ro/stiri-si-media/comunicate/proiect-european-implementat-de-politia-romana](https://www.politiaromana.ro/ro/stiri-si-media/comunicate/proiect-european-implementat-de-politia-romana)
• the lack of a prior Data protection impact assessment
• the lack of prior consultation with the national supervisory authority (ANSPDCP)
• the low weight of algorithm correctness - according to the contract award criteria mentioned in the Procurement Specification, the weight for “Search / comparison algorithm efficiency” is only 30%

All these aspects reinforce our fears that the IT solution, as it is presented in the Specification, will expose the data subjects to an imminent risk of violation of the right to privacy.

We asked for a number of clarifications³ from the contracting authority, however, the answer suggested that at the time of drawing up the Specifications⁴ the obligatory steps according to the national legislation were not followed. We emphasize that ignoring these aspects when designing the specifications, will inevitably have irreversible repercussions on the data subjects that may be affected by the facial recognition system.

In accordance with Article 32 of Law no. 363/2018, as well as with the Decision of the National Supervisory Authority no. 174 of October 18, 2018, the contracting authority (General Inspectorate of the Romanian Police) had the obligation

- performing a data protection impact assessment (DPIA);
- prior consultation with the National Supervisory Authority for Personal Data Processing

The contracting authority (General Inspectorate of the Romanian Police) could not confirm the existence of this assessment or the fulfillment of this obligation.

According to art. 11 of Law no. 363/2018, the adoption of a decision based exclusively on automatic processing, including the creation of profiles, which produces a negative legal effect for the data subject or which significantly affects it, is prohibited, unless the processing is expressly regulated by law, being provided adequate guarantees for the rights and freedoms of the data subject, including the right to obtain human intervention from the operator.

The contracting authority did not indicate the existence of an express regulation of the law that aims to use facial recognition systems nor adequate guarantees for the rights and freedoms of the data subject.

We have requested the requirements of the Contracting Authority regarding the functionalities of the facial recognition system that will ensure compliance with the provisions of art. 13 and art. 16-21 of Law no. 363/2018. The contracting authority did not indicate such requirements in the acquisition documentation.

According to the provisions of art. 25 of the General Regulation on Data Protection (EU Regulation 679/2016) establishing the obligation to ensure data protection from the moment of conception (“privacy by design”) and throughout the life of the system (“privacy by default”), the contracting authority had the obligation to establish appropriate technical and organizational measures from

the moment of elaboration of the Specifications of the procedure in question. **The contracting authority did not indicate such requirements contained in the acquisition documentation.**

According to the provisions of art. 33 of Law no. 363/2018, when discussing the use of new technologies, mechanisms or procedures that involve a high risk to the rights and freedoms of the data subjects, it is necessary to **consult the national supervisory authority. The contracting authority did not indicate the existence of a consultation with the supervisory authority.**

According to art. 49 of Law no. 363/2018, the interoperability of the systems of records of personal data is possible only with the prior consultation of the supervisory authority. **The contracting authority could not indicate the existence of a consultation with the supervisory authority.**

We emphasize that the Contracting Authority did not provide our requests with clear and complete answers as required by the public acquisition law, practically refusing to answer us by invoking the fact that our requests do not cover technical issues. Or, from our point of view, **appropriate technical and organizational measures** that the implementation of such a system involves, concern precisely technical issues.

Furthermore, the Contracting Authority mentions in the **response to the clarification request**5 that "**After the conclusion of the contract and the signing of the acceptance report without objections before the system goes into production, IGPR will comply with all rules and legal provisions**". From the analysis of the expression mode, we understand that the IGPR (the Contracting Authority) will acquire the facial recognition technology without complying with the legal requirements in force, and will assume compliance with the legislation in the subsequent phase of commissioning. Such an approach shows us that it is very unlikely that a functional system will comply with the legislation in force as long as at the time of acquisition the appropriate technical and organizational measures imposed by the legislation in force were omitted at the time of preparation of the Procurement Specification.

**Risks associated with facial recognition systems**

Some of the risks associated with this type of processing:

- **false matches** - wrong identification of persons;
- **discrimination** - face recognition systems have a much lower efficiency in the case of Black Male Adult (BME), women and especially children. These errors create and reinforce the categories discriminated on the basis of gender and race, with socially negative effects;
- **abuses** - without the existence of clear regulations regarding the conditions of use of such a system, its abusive use is very likely;
- **change of behaviour** - will determine the change of the behaviour of the people in order to comply with the general behaviour accepted by society. People will be afraid to participate in certain types of events for fear of not being associated with a certain category of people (sporting events, concerts, public manifestations, etc.).

---

The provisions of European law

In accordance with Art. 9 paragraph (1) of Directive 680, to the automatic processing operations for the unique identification of the individual and with the generation of automated individual decisions that can generate negative legal effects for data subjects in order to combat and elucidate the cases associated with identity theft, lost documents, identification of suspects who commit or intend criminal acts (terrorism, violent crime, etc.), GDPR requirements are not opposable, insofar as the data collected for the stated purposes will not be processed for purposes other than those falling under the Regulation.

Even if the requirements of Directive 680 do not have direct applicability for Member States such as the GDPR, in order to ensure the right to privacy in relation to the processing of personal data in the police sector, these needs are imperative.

In this sense, art. 10 of Directive 680/2016 expressly and without any interpretation states that: the processing of genetic data, the processing of biometric data for the unique identification of an individual[ ..... ] is authorized only when strictly necessary and subject to adequate safeguards for the rights and freedoms of the data subject and only when authorized by Union or national law.

In order to appreciate the conformity of this acquisition, the following questions are required:

- Art. 12-18, how the rights of the data subjects will be realized and to what extent they will be insured / restricted, including the period for which they will not be informed;
- Art. 22, which are the organizational and technical measures implemented by the authorized person, which apparently is of private law;
- Art. 24, which is the normative act that establishes the conditions for recording data processing: in particular, which would refer to: data recipients, categories of data subjects, eventual transfer to a third country, legal basis of processing, deadline for data deletion, general technical security measures provided.
- Art. 27, if the impact on data protection has been evaluated before processing the special category of data through the development of a new technology.
- Art. 28, if the Supervisory Authority has been consulted in advance, including what was its position on the case, specifying the essential aspects;
- Art. 36-37, if the transfer to third countries will be carried out and what will be the opposite situations;
- Art. 41, which is the Authority responsible for ensuring the protection of personal data in the case of such data processing operations and which are its effective competences.

It should be mentioned that, as CEDO states in its many decisions, the mere fact of the collection and recording by a public authority of the personal data - represents an interference in the private life, which can only take place if provided by the LAW and it is needed in a democratic state.

Other aspects that cannot be ignored:
According to the contract award criteria mentioned in the Procurement Specification, the weight for the "Efficiency of the search / comparison algorithm" is only 30%, being on the same level with the offer price, the rest of the evaluation factors regarding hardware characteristics that do not affect the accuracy of facial recognition software;

Also, another concern is the lack of requirements regarding the demonstration of the technical and professional capacity of the tenderer. Therefore, operators who will submit an offer will not have to prove that they have experience in implementing a similar solution or at least that the personnel who will handle the installation of the system and/or train the personnel of the contracting authority are qualified and have specific experience in such projects;

According to the specifications, the facial recognition system will be able to perform searches / checks / comparisons of the facial images from the police databases, associating them with those from the CCTV, webcam, mobile phones, social networks, ATM cameras. A monitoring that integrates all these systems that collect facial data, which may surprise people in the public as well as the private environment, is extremely invasive in the private lives of individuals. It is a processing disproportionate to the theoretical benefits that this system proposes, theoretical because this technology is still under development and for the moment it remains uncertain.

Examples regarding the implementation of facial recognition systems

1. South Wales (UK) police use automated facial recognition technology to prevent crime

The system was challenged and the judges decided⁶ that although the use of an automatic facial recognition system is an interference with the right to privacy, there is a legal basis for this, and the guarantees offered by the police regarding the respect of the rights and freedoms of the data subjects have been proportional.

Following this decision, ICO, the UK supervisory authority, said⁷ that "In the meantime, any police force or private organization using these systems should be aware that data protection legislation and guidelines still apply."

2. The use by the London Metropolitan Police (United Kingdom) of automatic face recognition technology for crime prevention

The London Metropolitan Police tested a facial recognition system between August 2016 and July 2018. According to data released by the London police⁸, during the system testing period, 104 alerts were triggered out of which 102 proved to be wrong, while only two were confirmed. That means a false match rate of over 98%.

---

Risk scenarios associated with the acquisition:

- The system will not be able to operate due to the lack of adequate technical and organizational measures required by the legislation in force. In other words, there is money thrown out the window.
- The system will not operate legally, and all persons who will be identified by this system will be able to challenge in court its legality.
- Persons subjected to this type of mass monitoring will complain against using this system invoking the violation of their rights and freedoms;
- False matches will generate the distrust of Romanians in the effectiveness of this system, thus further diminishing the confidence in the Romanian Police's ability to ensure an adequate degree of safety.

We believe that the implementation of such type of technology must be tightly regulated and subject to strict control in order to avoid possible abusive uses or which would have the effect of violating the rights and freedoms of the data subjects and at the same time diminishing the confidence of the population in the Romanian Police institution, whose slogan is: "Safety and trust".

In order to comply with the technical solution, we request the analysis of the following proposed actions:

1. cancellation of the acquisition procedure in question;
2. identification or elaboration of a legal framework that expressly regulates such a mass monitoring system;
3. conducting an evaluation of the impact of data processing for this type of processing;
4. consulting with civil society on the use of a facial recognition system;
5. consulting the DPA on the result of the evaluation of the impact of the processing in order to establish together the appropriate measures that will be put in place to protect the rights, freedoms and legitimate interests of the data subject;
6. drafting a new Procurement Specification containing express requirements regarding the technical and organizational measures that the system must include from the moment of conception;
7. establishing at least 70% of the weight of the selection criterion on “The effectiveness of the search / comparison algorithm”, which is by far the most important aspect of this system;
8. imposing selection criteria regarding the demonstration of the technical and professional capacity by requesting the demonstration of the existence of a similar experience by implementing a similar system and requesting recommendations issued by the beneficiaries, as well as requesting the evidence regarding having a specialist in the privacy data that will assist throughout the implementation period of the system and the training of the personnel of the contracting authority.
Conclusion

We reiterate the fact that we support the introduction of a new technology for **increasing the degree of combating and elucidating the crimes** that respect the right to privacy of the data subjects as well as the other criteria provided in the law. We emphasize that the interoperability of personal data must be based on transparency and respect for the principles of personal data collection, so that citizens can be confident that their data are processed properly, without the risk of an imbalance.

Therefore, we ask you to make sure that you have taken all the necessary steps to enable this system to become functional and its effectiveness is optimal, in accordance with the legal provisions, so that its purpose is achieved without prejudice to the rights and of people’s freedoms.

**Signatories:**

Association of Specialists in Privacy and Data Protection ([www.ascpd.ro](http://www.ascpd.ro))

*Marius Dumitrescu, President*

Association for Technology and Internet – ApTI ([www.apti.ro](http://www.apti.ro))

*Bogdan Manolea, Executive Director*

Association for the Protection of Privacy ([www.privacy.md](http://www.privacy.md))

*Sergiu Bozianu, President*

Association for the Respect of Human Rights ([www.ardom.ro](http://www.ardom.ro))

*Maria Pop, President*