



WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Philippe RENAUDIÈRE
Data Protection Officer
European Commission
Rue de la Loi, 200
B-1049 Brussels

07 AOUT 2017

Brussels,
WW/EF/ktl D (2017)1691 C 2017-0509
Please use edps@edps.europa.eu for all
correspondence

Dear Mr Renaudière,

Please be informed that, by email of 22 May 2017, Mr Zioga submitted us a consultation under Article 27(3) of Regulation (EC) 45/2001¹ (the Regulation). This consultation concerned the processing of fingerprint data for the purpose of a research study carried out by the Joint Research Centre (JRC).

After careful examination we consider that the case in question is **not subject to prior checking** for the reasons explained below.

1. Facts - Description of the processing operation

The processing operation, as notified by the controller to the Data protection Officer (DPO), concerns the processing of fingerprint data for the purpose of a research study carried out by the Joint Research Centre (JRC). The research project is called FLARE (fingerprint laser recognition).

The aim is to carry out research on the next generation three-dimensional (3D) fingerprint laser recognition. It will constitute a step forward from the existing 2D fingerprint recognition, which gives some error rate.

FLARE will thus explore the possibility of using a new generation of very accurate 3 D laser-based sensing technology that will acquire (in a contactless environment) the full 3 D-fingerprint surface.

¹ OJ L 8, 12.1.2001, p. 1.

The project will be carried out at the premises of the JRC based on a sample of 50 staff members that will voluntarily provide their fingerprints and 4 (four) fingers per subject, 5 (five) samples per finger and 3 (three) sensing speeds.

In total 60 (sixty) samples will be collected and the experiment session will last around 15 minutes. There are no risks or discomforts connected to the research. According to the documents provided, the use of laser diode within the acquisition device complies with security measures.

The persons participating in the project will do it on a voluntary basis, based on a call for expression of interests. Some of the persons, however, are contacted on an *ad hoc* basis².

It is explicitly mentioned that there is no adverse measure if data subjects do not want to participate and they may withdraw consent at any moment.

The purpose of the processing operation is to conduct research exclusively and the legal basis for the processing operation is consent, thus Article 5 (d) of Regulation 45/2011.

As to the security of the data, fingerprints will be stored in a computer with no access to internet. In addition, they will be stored in an encrypted database. Data will also be pseudonymised, meaning that identification of individuals can only be done with additional information. The fingerprints thus will not be directly connected with the identity of the data subject: each data subject is assigned a numerical identifier and the fingerprints will be stored with this numerical identifier. The link between the numerical identifier and the fingerprint will be indicated in a notebook stored in a restricted area of the laboratory.

Data subjects will obtain both a privacy statement and a declaration on informed consent.

2. Analysis

Article 27 (1) of the Regulation provides that processing operations likely to present specific risk to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes shall be subject to prior checking by the EDPS. In this sense, Article 27(2) (a) of the Regulation provides that processing of data relating to health falls within this category.

In principle, processing fingerprints does not imply processing health data. The reason is that, although potentially possible³, there is certain difficulty in deducing information about the health status of a person out of a fingerprint sample. In addition, the purpose of the processing operation has neither a direct nor indirect link with the health of persons as it concerns the testing (research) of a new technology.

However, according to some studies, the fingerprint images can reveal some ethnic information about the individual.⁴ Article 10 of the Regulation states that processing personal data relating to

² According to the complementary information sent, 'other colleagues outside the unit that are part of the personal acquaintances of the main researchers in Ispra were asked if they wanted to participate in the project in a strictly voluntary basis as well.'

³ Point 29 de l'avis 17/2008 Commission de la protection de la vie privée du 9 avril 2008 avis d'initiative relatif au traitement des données biométriques dans le cadre de l'authentification de personnes (A/2008/017).

⁴ See footnote 15 of Opinion 3/2012 on developments in biometric technologies of the Article 29 Data Protection Working Party, as adopted on 27th April 2012.

the ethnical or racial origin is prohibited.⁵ Since the present processing operation does not have either the purpose or the effect of evaluating the ethnic origin of the data subjects it cannot be considered that it falls within this special category.

Nevertheless, it should be examined whether the processing operation can still be subject to prior checking given that Article 27 (1) of the Regulation covers all processing operations that may create risks to the rights and freedoms of the subject.

Firstly, the sole purpose of the processing operation is to carry out research by a research directorate of the Commission. According to some opinions of the EDPS when the purpose of the processing operation is merely to carry out research and there are a number of safeguards in place the processing operation should not be subject to prior checking.⁶

Secondly, the lawfulness is ensured by the explicit consent that is given by the data subjects. Consent is a core issue in the use of fingerprints for uses other than in law enforcement.⁷ An open call for interest will ensure that the consent is given freely given, specific and informed, as there is no obligation to participate. Further, data subjects may withdraw consent at any time; they receive a document entitled *informed consent* where it is stated that “*your refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You may withdraw your consent at any time and discontinue participation without penalty. ...*”

Nevertheless, according to the complementary information received, other colleagues may be asked to participate on a voluntary basis outside the call for expression of interest. The controller should ensure that these persons participate under the same conditions as those replying to the call for expression of interests, this is, on a voluntary basis and with the possibility to withdraw consent. Such equality of conditions is necessary to ensure that the consent is valid, this is, freely given, specific and informed.

Thirdly, the retention period is equivalent to the duration of the research and seems proportionate, given that the data will not be kept for more than two years.

Fourthly, the security measures taken in order to guarantee compliance with Article 22 of the Regulation are appropriate since data are pseudonymised and the database where they are stored is, in addition, encrypted. The EDPS considers best practice that data are stored in a computer physically disconnected from the network and not accessible from the outside world.

However, security could be reinforced in the field of pseudonymisation of the data. The link used in the pseudonymisation of data could be stored in a separate software/database instead of in a simple notebook stored in a restricted place of the laboratory. It may well be that the organizational security measures put in place by the controller for storing the notebook are sufficient. In any case the EDPS recommends the **controller to implement** the appropriate technical and **organizational** security measures appropriate to mitigate the risk (and to be able to justify these choices).

⁵ For photos, we said that they don't fall under 10, unless you use them for the purpose of such evaluations; should be the same reasoning here (WP29 opinion 02/2012 in footnote + EDPS 2013-0717).

⁶ See for example ‘prior checking notification regarding social biking: a field study on physical activity and social networks’ (EDPS case 2017-0080) of 8 March 2017.

⁷ See paragraph 4.4.2 of the Opinion 3/2012 on developments on biometric technologies, footnote 4.

3. Conclusion

Although processing fingerprint data for the purpose of a research study carried out by the JRC does not present specific risks to the rights and freedoms of data subjects under Article 27 of the Regulation, the EDPS had identified two recommendations to make. The EDPS expects implementation of the following recommendations, but does not require documentary evidence:

1. Given that consent is a core issue in the present processing operation, the controller should ensure that participants are all on equal footing as regards to free, valid and unambiguous consent;
2. Given that security measures are crucial in the present processing operation, the controller should ensure that the technical/organizational measures taken in the field of pseudonymisation are appropriate to the risk encountered.

In the light of the accountability principle, the EDPS expects JRC to implement the above recommendations accordingly and has therefore decided to **close case 2017-0509**.

Wojciech Rafał WIEWIÓROWSKI



P.O.

Cc: Ms. Viktoria ZIOGA, European Commission