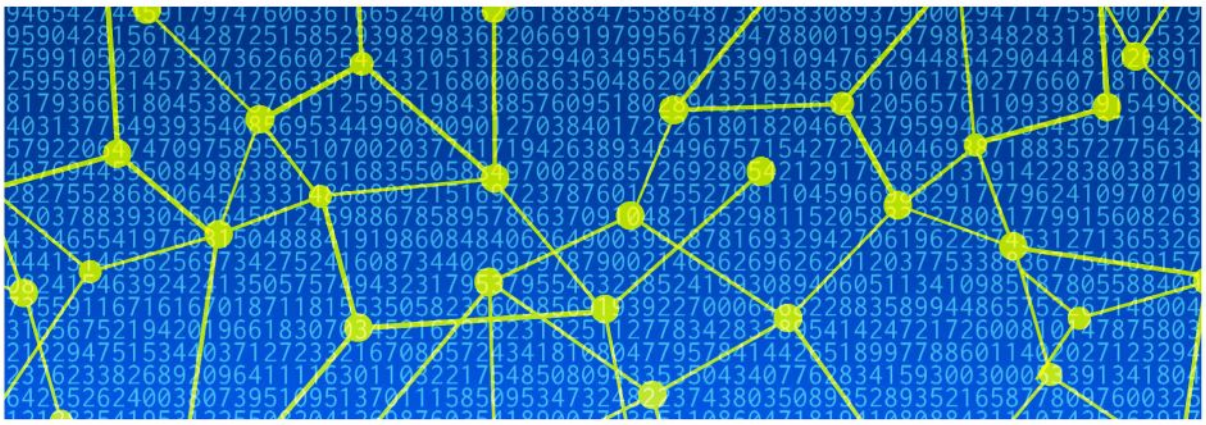

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Opinion 7/2018

on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents

EDPS

10 August 2018

The European Data Protection Supervisor ("EDPS") is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. While the EDPS supports the objectives to enhance the security of ID cards and residence documents, thus contributing to a more secure Union overall, he considers that the Proposal should be improve in certain key aspects so as to ensure compliance with data protection principles.

Executive Summary

This Opinion outlines the position of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

In this context, the EDPS observes that the Commission has clearly chosen to prioritise the free movement aspects of the Proposal and to treat the security-related objective as corollary. The EDPS remarks that this might have an impact on the analysis of necessity and proportionality of the elements of the Proposal.

The EDPS supports the objective of the European Commission to enhance the security standards applicable to identity cards and residence documents, thus contributing to security of the Union as a whole. At the same time, the EDPS considers that the Proposal does not sufficiently justify the need to process two types of biometric data (facial image and fingerprints) in this context, while the stated purposes could be achieved by a less intrusive approach.

Under the EU legal framework, as well as within the framework of Modernised Convention 108, biometric data are considered sensitive data and are subject to special protection. The EDPS stresses that both facial images and fingerprints that would be processed pursuant to the Proposal would clearly fall within this sensitive data category.

Furthermore, the EDPS considers that the Proposal would have a wide-ranging impact on up to 370 million EU citizens, potentially subjecting 85% of EU population to mandatory fingerprinting requirement. This wide scope, combined with the very sensitive data processed (facial images in combination with fingerprints) calls for close scrutiny according to a strict necessity test.

In addition, the EDPS acknowledges that, given the differences between identity cards and passports, the introduction of security features that may be considered appropriate for passports to identity cards cannot be done automatically, but requires a reflection and a thorough analysis.

Moreover, the EDPS wishes to stress that Article 35(10) of the General Data Protection Regulation (hereinafter *"GDPR"*)[1] would be applicable to the processing at hand. In this context, the EDPS observes that the Impact Assessment accompanying the Proposal does not appear to support the policy option chosen by the Commission, i.e. the mandatory inclusion of both facial images and (two) fingerprints in ID cards (and residence documents). Consequently, the Impact Assessment accompanying the Proposal cannot be considered as sufficient for the purposes of compliance with Article 35(10) GDPR. Therefore, the EDPS recommends to reassess the necessity and the proportionality of the processing of biometric data (facial image in combination with fingerprints) in this context.

Furthermore, the Proposal should explicitly provide for safeguards against Member States establishing national dactyloscopic databases in the context of implementing the Proposal. A

provision should be added to the Proposal stating explicitly that the biometric data processed in its context must be deleted immediately after their inclusion on the chip and may not be further processed for purposes other than those explicitly set out in the Proposal.

The EDPS understands that using biometric data might be considered as a legitimate anti-fraud measure, but the Proposal does not justify the need to store two types of biometric data for the purposes foreseen in it. One option to consider could be to limit the biometrics used to one (e.g. facial image only).

Moreover, the EDPS would like to underline that it understands that storing fingerprint images enhances interoperability, but at the same time it increases the amount of biometric data processed and the risk of impersonation in case of a personal data breach. Thus, the EDPS recommends to limit the fingerprint data stored on the documents chip to minutiae or patterns, a subset of the characteristics extracted from the fingerprint image.

Finally, taking into account the wide range and potential impact of the Proposal outlined above, the EDPS recommends setting the age limit for collecting children's fingerprints under the Proposal at 14 years, in line with other instruments of EU law.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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)[2],

Having regard to Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[3], and in particular Articles 28(2), 41(2) and 46(d) thereof,

Having regard to Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[4],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. On 17 April 2018, the European Commission (hereinafter *"the Commission"*) issued the Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement[5] that aims to improve the security features of EU citizens' identity cards and non-EU family members' residence cards (hereinafter *"the Proposal"*).

2. This proposal for a Regulation is part of the Action Plan of December 2016 "*to strengthen the European response to travel document fraud"* (hereinafter *"the Action Plan of December 2016"*)[6], in which the Commission identified actions to address the issue of document security, including identity cards and residence documents, in the context of recent terrorist attacks in Europe.

3. ID cards play an important role to secure the identification of a person for administrative and commercial purposes, which has been underlined by the Commission in its Communication adopted on 14 September 2016 *"Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders"*[7] . The need to improve the security of these documents was also highlighted in the EU Citizenship Report 2017.

4. Part of the EDPS` mission is to advise the Commission services in the drafting of new legislative proposals with data protection implications.

5. The EDPS welcomes that he had already been consulted informally by the European Commission on the draft Proposal and was given the opportunity to provide input on data protection aspects.

2. OBJECTIVES AND CONTEXT OF THE PROPOSAL

6. The EDPS notes that the Proposal places great emphasis **on security and the fight against terrorism and organised crime**. The Explanatory Memorandum begins by stating that *"[e]nsuring the security of travel and identity documents is a key element in the fight against terrorism and organised crime"*. It further stresses that *"[e]nhanced document security is an important factor in improving the security within the EU and its borders and in supporting the move towards an effective and genuine Security Union"*[8]. The main objective of the Proposal is to *"strengthens the security standards applicable to identity cards issued by Member States to their nationals and to residence documents issued by Member States to Union citizens and their family members when exercising their right to free movement"*[9].

7. The Impact Assessment accompanying the Proposal also mentions other objectives of the Proposal, including *"to reduce document fraud, to improve the acceptance and authentication of the ID and residence documents and improve the identification of people based on them."* Moreover, *"to raise awareness among citizens, national authorities and the private sector about the documents issued, and the right to free movement linked to them."* Finally, *"to simplify daily life for EU citizens, cut red tape and lower costs for both citizens and private and public entities, by reducing administrative barriers… related to the use of ID cards and residence documents"*[10].

8. The EDPS notes that the legal basis for the Proposal is Article 21(2) TFEU. This provision states that, *"[i]f action by the Union should prove necessary to attain [the free movement of persons] objective, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may adopt provisions with a view to facilitating the exercise of"* free movement rights. **The EDPS observes that the Commission has clearly chosen to prioritise the free movement aspects of the Proposal and to treat the security-related objective as corollary. The EDPS observes that this might have an impact on the analysis of necessity and proportionality of the elements of the Proposal** (see below)**.**

9. At present, the Citizens' Rights Directive (EU) 2004/38[11] **does not regulate the format and minimum standards for identity cards nor does not provide for specific standards** as regards **residence documents** issued to citizens of the Union and their non-EU family members. Consequently, the Directive (EU) 2004/38 **does not require** that the identity cards, residence documents delivered to citizens of the Union or residence cards delivered to non-EU family members of EU citizens **contain biometric data** such as a facial image of the holder of the card and/or fingerprints in interoperable formats.

10. The Proposal aims to strengthen the security of the EU citizens' identity cards and the non-EU family members' residence cards by adding the **compulsory inclusion of biometric data (two fingerprints and a facial image) in identity cards** delivered to their citizens by Member States and **in residence cards for family members** who are not nationals of a Member State. In this respect, the Proposal provides that the identity cards issued by Member States shall be produced in ID-1 format and comply with the minimum security standards set out in ICAO Document 9303 (seventh edition, 2015). According to the ICAO Document 9303 (seventh edition, 2015) (hereinafter *"the ICAO Document"*) the biometric data will be stored to be used with facial, fingerprint or iris recognition systems[12].

11. As regards the **residence cards for family members** who are not nationals of a Member States, Article 7(1) of the Proposal states that: *"[w]hen issuing residence cards to family members of Union citizens who are not nationals of a Member State, Member States shall use the same format as established by the provisions of Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals*". Today, Article 5 of the Regulation (EU) 1030/2002[13], which lays down a uniform format for residence permits for third country nationals, provides that the Regulation (EU) 1030/2002 does not apply to, inter alias, *"third-country nationals who are members of the families of citizens of the Union exercising their right to free movement (...)"*. As a result, at present Article 4a of the Regulation (EU) 1030/2002, which requires to include in the residence permits for third country nationals a facial image and two fingerprints as biometric identifiers, does not apply to the third-country nationals who are members of the families of citizens of the Union.

12. **The EDPS supports the objective of the European Commission to enhance the security standards applicable to identity cards and residence documents, thus contributing to security of the Union as a whole.** At the same time, as set out in detail below, **the EDPS considers that the Proposal does not sufficiently justify the need in this context to process two types of biometric data (facial image and fingerprints) in this context, while the stated purposes could be achieved by a less intrusive approach.**

3. PROPORTIONALITY AND NECESSITY OF THE PROCESSING OF BIOMETRIC DATA

3.1. Sensitive nature of biometric data

13. The EDPS would like to emphasise that **the processing of biometric data constitutes a limitation on the fundamental rights to privacy and personal data protection** and, like any interference with a fundamental right, **must comply with the criteria set out in Article 52(1) of the Charter of Fundamental Rights of the European Union (hereinafter *"the Charter"*)**[14]. In addition to being provided for by law, any limitation must respect the essence of the right and, subject to the principle of proportionality, be necessary and genuinely meet objectives recognised by the Union or the need to protect the rights and freedoms of others.

14. Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows those individuals to be identified with precision[15]. In the EU legal order, **biometric data are defined as personal data** resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which **allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data**[16]. **Under the EU legal framework**[17]**, as well as within the framework of Modernised Convention 108**[18] **biometric data are considered as one of the special categories of personal data**[19] **and are subject to special protection**: their processing is prohibited in principle and there are a limited number of conditions under which such processing is lawful. This specifically applies to biometric data processed for the purpose of identifying a person. **The EDPS stresses that both facial images and fingerprints that would be processed pursuant to the Proposal would clearly fall within this sensitive data category**.

15. Consequently, the EDPS stresses the need to ensure that the processing of biometric data pursuant to the Proposal remains **limited to what is strictly necessary to achieve its stated objectives.** Moreover, given the particularly sensitive nature of biometrics data, it will be necessary to provide for **appropriate safeguards** (see further below).

3.2. Wide-ranging scope and impact of the Proposal

16. The EDPS would like to recall that, as provided in the EDPS Necessity Toolkit[20] **necessity is a fundamental principle when assessing the restriction of fundamental rights**, such as the right to the protection of personal data. According to case-law, because of the role the processing of personal data entails for a series of fundamental rights, the limiting of the fundamental right to the protection of personal data must be strictly necessary. **Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation.** Necessity is also fundamental when assessing the lawfulness of the processing of personal data. The processing operations, the categories of data processed and the duration the data are kept shall be necessary for the purpose of the processing.

17. The Proposal does not require Member States to introduce identity cards or residence documents where they are not provided for under national law, nor does it affect the competence of the Member States to issue other residence documents under national law outside the scope of Union law[21]. Thus, **the new rules provided in the Proposal will affect these Member States that already issue identity cards or residence documents**, whether they are compulsory or not.

18. In this context, it is worth underlining that Denmark and the United Kingdom do not issue identity cards at all. Out of the 26 Members States who do issue identity cards, possession of such a card is compulsory only in the 15 Member States[22]. Identity cards issued by 13 Member States currently do not include any biometrics[23]. In conclusion, **up to 370 of the 440 million citizens in 26 Members States would be affected by the Proposal, which corresponds to almost 85% of the EU's 440 million citizens**[24]. The 370 million citizens is the *"total number of potential ID card holders in 26 Member States"*[25], 175 million of

whom would be subject to a new obligation to provide fingerprints for identity cards[26] (16 Member States). The remaining 195 million of EU citizens, who are already under an obligation to possess an identity card according to existing national law, would also be affected by the new requirements – once introduced at EU level, it would not be possible for Member States to reverse requirements for fingerprints in identity cards through national measures alone.

19. Consequently, **the EDPS considers that the Proposal would have a wide-ranging impact on up to 370 million EU citizens, potentially subjecting 85% of EU population to mandatory fingerprinting requirement. This wide scope, combined with the very sensitive data processed (facial images in combination with fingerprints) calls for close scrutiny according to a strict necessity test.**

3.3. Justification for the Proposal: national identity cards vs. passports and the impact on the free movement

20. The EDPS notes that the Proposal attempts, on multiple occasion, to present national identity cards issued by EU Member States to their citizens as **legally and functionally equivalent to passports**. The Explanatory Memorandum of the Proposal states[27] that the inclusion of the two biometric identifiers will "*align the level of document security of identity cards of EU citizens and residence cards issued to third country family members to the standards of, respectively, passports issued to EU citizens and residence permits issued to third country nationals who are not family members of EU citizens.*"

21. The Proposal refers to identity cards and passports almost interchangeably in relation to exercising the right of free movement by EU citizens (and their family members) and introduces requirements equivalent to those applicable to passports. According to the Council Regulation (EC) 2252/2004, currently **the passport and travel documents** issued by the Member States **shall include a highly secure storage medium**, which shall **contain a facial image and two fingerprints** taken flat in interoperable formats. In consequence, the Proposal introduces the compulsory inclusion of a facial image and two fingerprints as biometric identifiers into the residence cards that are issued by the Member States to family members of Union citizens.

22. In this context, **the EDPS supports the Commission's objective to facilitate free movement**. **Nevertheless, the EDPS notes that the two types of documents - identity cards and passports - are in fact very different, both from the legal point of view and in their practical use.** Even where used as travel documents in the free-movement context, national identity cards, unlike passports, can only be used to travel to EU Member States and these third countries, which allow EU citizens to travel using their national identity cards. In this context, EDPS questions the added value of including biometric data in the identity cards as they are not routinely checked when traveling between the EU Member States.

23. Even more importantly, **identity cards have a variety of uses that goes far beyond the exercise of the right to free movement** linked to EU citizenship, ranging from interactions

with a citizen's home country administrations, through interactions with a variety of actors from across the private sector (banks, airlines etc.). Furthermore, according to the Impact Assessment accompanying the Proposal, around 15 million EU citizens reside in another EU Member States, while 11 million work in another Member State[28]. The EDPS concludes that, for the vast majority of EU citizens the primary functions of identity cards are not directly linked to freedom of movement. By far not all EU citizens potentially affected by the requirements of the proposal to have their fingerprints included in national identity cards can be assumed to exercise their free movement rights. On the contrary, mobile EU citizens constitute a small minority of those potentially affected by the Proposal. Moreover, even those who do exercise their free movement rights in practice, can and often do so on the basis of a passport, not an identity card. **The justification for the Proposal** put forward by the Commission **is therefore not entirely convincing**.

24. The Proposal also refers to the need to combat document fraud, in particular forgery of documents or false representation of material facts concerning the right of residence. It is unclear to what extent enhanced security features including biometrics could help address the issue of *"false representation"*. At any rate, as mentioned in the Impact Assessment accompanying the Proposal, **in the years 2013-2017** the European Border and Coast Guard Agency (FRONTEX) has collected statistics on fraudulent identity cards and residence documents and **it detected only 38.870 fraudulent identity cards[29].**

25. Furthermore, as stated in the Annex 6 to the Impact Assessment, the number of persons using fraudulent identity cards and residence documents arriving from third countries **decreased by 11% in 2015 (8 373)**[30]. This trend is also confirmed by the 2017 FRONTEX Risk Analysis[31], where the number of persons using fraudulent documents **further decreased in 2016 to 7 044.** The trend specifically for **ID cards** is similar to fraudulent documents overall, with a **decrease in detections in 2016** [32].

26. In the EDPS view, **this relatively low number[33]** of fraudulent identity cards and residence documents and the fact that **the number of persons** using fraudulent identity cards and residence documents arriving from third countries **is gradually decreasing,** do not in itself justify the far-reaching solutions put forward in the Proposal.

27. Consequently, **the EDPS considers that, given the differences between identity cards and passports, the introduction of security features that may be considered appropriate for passports to identity cards cannot be done automatically but requires a reflection and a thorough analysis**.

3.4. Need for a Data Protection Impact Assessment

28. The EDPS also notes that pursuant to Article 35(1) of the General Data Protection Regulation (hereinafter *"GDPR"*)[34], a Data Protection Impact Assessment (hereinafter *"DPIA"*) shall be conducted before a processing activity that is *"likely to result in a high risk to the rights and freedoms of natural persons"* takes place. The EDPS considers that this requirement is fully applicable in the context of the Proposal. The **DPIA should cover all processing operations envisaged for both categories of biometric data covered, i.e.**

facial images and fingerprints. In particular, the DPIA should include an assessment of the risks to the rights and freedoms of the data subjects as well as measures envisaged to address these risks such as safeguards and security measures.

29. The EDPS wishes to stress in this context that **Article 35(10) of the GDPR would be applicable to the processing at hand** (which would have legal basis in Union law, i.e. the Proposal). Consequently, **unless the DPIA is carried out in the context of the adoption of the Proposal, Member States will be under the obligation to carry it out at the later stage.** In this context, **the EDPS observes that the Impact Assessment accompanying the Proposal does not appear to support the policy option chosen by the Commission,** i.e. the mandatory inclusion of both facial images and (two) fingerprints in ID cards (and residence documents).

30. Indeed, when considering the different Policy Options ID, the Impact Assessment states that: ***"Under options ID 2) and ID 3) citizens will be required to provide their fingerprints when ID cards are requested.*** *This obligation interferes with the fundamental rights to privacy and data protection. While in the Schwarz case*[35] *the CJEU held that the interference with regard to passports is proportionate to the objective of maintaining security,* ***in the context of ID cards the threshold for satisfying the necessity test may be higher, because ID cards are compulsory in some Member States in which fingerprints are not currently collected"***[36]***.***

31. Following the comparison of policy options, the Impact Assessment indicates Option ID 1) as the most suitable to promote the objectives of improving security at borders and internally within Member States, and freedom of movement. Remarkably, that Option ID 1) preferred by the Impact Assessment report would involve a *"****mandatory RFID chip including biometrics (facial image mandatory, fingerprints optional)****"*[37]. In other words, the policy option supported by the Impact Assessment accompanying the Proposal would include fingerprints **optionally, and not as a compulsory requirement.**

32. Surprisingly, the Commission decided, despite the result of the Impact Assessment that accompanying the Proposal, to include the mandatory inclusion of fingerprints in identity cards in the Proposal. In the Explanatory Memorandum of the Proposal is it stressed that: ***"Mandatory fingerprints were added to the preferred option for identity cards in order to further increase effectiveness in terms of security.*** *The inclusion of two biometric identifiers (facial image, fingerprints) will improve the identification of persons and align the level of document security of identity cards of EU citizens and residence cards issued to third country family members to the standards of, respectively, passports issued to EU citizens and residence permits issued to third country nationals who are not family members of EU citizens."*[38]

33. **Consequently, the Impact Assessment accompanying the Proposal cannot be considered as sufficient for the purposes of compliance with Article 35(10) GDPR.** Therefore, **the EDPS recommends to reassess the necessity and the proportionality of the processing of biometric data (facial image in combination with fingerprints) in this context.**

4. PROCESSING OF BIOMETRIC DATA: NECESSARY SAFEGUARDS

34. Article 3(3) of the Proposal would require identity cards issued in the EU to include **a highly secure storage medium** which shall **contain a facial image of the holder of the card and two fingerprints in interoperable formats.**

4.1 Purpose specification

35. The purpose limitation principle[39] requires that personal data must be collected for specified, explicit and legitimate purposes and it cannot be further processed in a manner which is incompatible with those purposes. In this context, **the EDPS welcomes that Article 10 of the Proposal exhaustively lists the purposes for which the personal data will be processed**.

36. Furthermore, according to Article 10(3) of the Proposal the processing of the biometric data included in the ID cards and residence documents is allowed for two purposes:

> *"for verifying:*
> *a) the authenticity of the identity card or residence document;*
> *b) the identity of the holder by means of directly available comparable features when the identity card or residence document is required to be produced by law.".*

37. As a preliminary remark, the EDPS observes that **the match between biometric data stored in the chip of the document** and **biometric data provided by the document holder** is only **a proof that the document belongs to the document holder**. That match does not as such constitute a proof of identity unless the document has been also proved to be authentic.

38. The authenticity of the document could be proved by a **match between biometric data stored in the chip** and **a copy of the biometric data collected at enrolment**. However, the creation of a nationals dactyloscopic databases, which is not anyway envisaged in the Proposal, should be avoided. Thus, the only option would be to check the matching of the data stored in the chip with the data printed in the document. The integrity of the data stored in the chip relies on the digital certificate that is also stored in the chip. Digital certificates have an expiry date and could be revoked by the issuing authority. Thus, any verifying system would need an Internet connection or an alternate method to update its certificate revocation list.

39. It has to be acknowledged that using biometric data reduces the likelihood of successfully forging a document, so it may be considered as a legitimate anti-fraud measure. However, the practical implementation of an authentication procedure based on the biometric data stored in the identity cards is a complex and long term project. Such a project is not

mentioned anyway in the Proposal and without it the storing of biometric data can't achieve its intended purpose.

40. Furthermore, the Action Plan of December 2016 lays down that ***"[i]n order to check the electronic components of e-passports and e-residence permits, the authorities need the Member State that has issued the document to provide them with the requisite certificates"***[40] so that they can access the fingerprints stored on the chip. The systematic electronic checking of the chip data would lead to the detection of the most common cases of document fraud, such as manipulations of the photo of the holder. **Unfortunately, not all Member States exchange their certificates**. The Action Plan of December 2016 contains an action foreseeing that the Commission would *"provide for a regularly updated list of certificates needed for the electronic authentication of travel documents during the third quarter of 2017"*[41]. However, the Impact Assessment accompanying the Proposal affirms that *"the keys to access data change over time and they are not always communicated immediately to the relevant national authorities"*[42].

41. **The EDPS also notes that the Impact Assessment accompanying the Proposal explicitly recognises that it is difficult to justify the necessity and proportionality of a restriction of the fundamental right to personal data protection envisaged in the Proposal**, in particular as regards the inclusion of fingerprints in the identity cards issued by Member States to their nationals. It highlights that as regards the inclusion of fingerprints, account has to be taken of the case law of the Court of Justice. In this context, in the *Schwarz case*[43] the Court concluded that although the taking and storing of fingerprints in passports constitutes an infringement of the rights to respect for private life and the protection of personal data, the inclusion of fingerprints in passports is lawful given the general objective of preventing *"illegal entry into the European Union"*[44]. However, the Impact Assessment recognises that ***"given that the ID cards serve more purposes than crossing the border and given the different traditions in Member States for the use of ID cards, it is not self-evident that the same conclusion could be drawn"***[45].

42. Furthermore, the EDPS emphasises that the processing of personal data must be limited to the legitimate purpose for which that personal data was originally collected from the data subject. In particular, the proposal **should explicitly provide for safeguards against Member States establishing national dactyloscopic databases** in the context of implementing the Proposal. A provision should be added to the Proposal stating explicitly that **the biometric data processed in its context must be deleted immediately after their inclusion on the chip** and may not be further processed for purposes other than those explicitly set out in the Proposal.

4.2 Data minimisation

43. The EDPS wishes to stress that **one of the key principles of EU data protection law is data minimisation**. According to this principle, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed[46].

44. While biometrics techniques have inherent advantages over traditional personal identification techniques, the problem of ensuring the security and integrity of the

biometrics data is critical. For example, if a person's biometric data (e.g., his/her fingerprint image) is stolen (e.g. illegally accessed and copied), it is not possible to replace it, unlike replacing a stolen or lost credit card, a paper identity card, or a password. A biometrics-based verification system works properly only if the verifier IT system can guarantee that the biometric data came from the legitimate person at the time of enrolment.

45. Against this background, fingerprint recognition technologies can be divided in three classes[47]:
    - those that store and compare **images** of fingerprints
    - those that store and compare **minutiae**, a subset of the characteristics extracted from fingerprint images
    - those that store and compare **patterns** extracted from fingerprint images.

46. The ICAO Document[48] requires the storage of the images of the fingerprints to ensure interoperability among the different types of fingerprint recognition technologies. There are standards that allow fingerprint recognition systems of different vendors to be interoperable amongst their class, but the fingerprint recognition systems are not interoperable between classes.

47. Storing fingerprint images allows the calculation of subsets of its characteristics while the opposite is not possible. Having the image of the fingerprint stored in the documents chip allows Member States that opted for any class of fingerprint recognition technology to use the biometric data. However, if the chip stored a minutiae, a Member State that deployed an image based fingerprint technology could not use the biometric data, as fingerprint images can't be obtained from minutiae. At the same time, in case of a security breach the fingerprint image stored on a lost or stolen identity document could be accessed by criminals and used to cast a fake set of fingerprints allowing to impersonate the identity card owner.

48. **The EDPS understands that storing fingerprint images enhances interoperability**, but at the same time **it increases the amount of biometric data processed and the risk of impersonation in case of a personal data breach**. Therefore, **the EDPS recommends to limit the fingerprint data stored on the documents chip to minutiae or patterns, a subset of the characteristics extracted from the fingerprint image**.

49. **Furthermore, EDPS considers that the processing of two different types of biometric data (facial image mandatory, fingerprints mandatory) foreseen in the Proposal is not justified, taking the stated objectives into account.** The purposes foreseen in Article 10(3) of the Proposal can be achieved with just one type biometric data. The Proposal does not explain if both types of biometric data should be checked to ascertain the identity of the holder or not.

50. Double checking on biometric data raises its own risks, associated to the ratio of false negatives (a failure result in a verification process that should have ended successfully) of the given technology (fingerprint or facial image). Making checks on fingerprints and facial

images could lead to situations in which the facial image check is successful while the fingerprint check fails or the other way around. Even if the percentage of false negatives for a certain biometric recognition technology is low, it could affect to a significant number of individuals when applied to a very large population like in the present case. Finally, it is possible that both types of biometric data are not going to be used, In this situation, only the one that is going to be used should be stored.

51. Article 3(1) of the Proposal sets the minimum security standards envisaged in the ICAO Document. Details of the required, recommended and optional security measures are defined in the part 11 (Security mechanisms) of the ICAO document. In the section 3.1 it is stated that *Passive Authentication* is the only required measure for the chip. According to the ICAO document, that measure does not prevent an exact, copy or IC substitution and neither prevents skimming[49]. In the section 3.1 it is stated that *Basic Access Control* is the only required measure for the verifying system. According to the ICAO document, that measure does not prevent an exact copy or IC substitution although it requires also copying of the conventional document and adds complexity. The EDPS considers that, if biometric data of 85% of the EU population are to be stored on identity cards, the Proposal should increase the minimum requirements to avoid this risks.

52. According to this Proposal anyone with access to an identity card and a reader that fulfils the standards set out in the ICAO document could access the biometric data of an individual by just having access to the document, even if the biometric data are not going to be used to check the identity of the holder by the third party.

53. Consequently, the mandatory inclusion of fingerprints the EU citizens' identity cards as foreseen in **the Proposal is not in line with the principle of data minimisation**, according to which a data controller should limit the processing of personal data to what is relevant and necessary to accomplish a specified purpose.

54. Nevertheless, **the EDPS wishes to stress that security printing techniques,** like the use of holograms or watermarks, **do not involve the processing of personal data but may allow preventing the forgery and verifying the authenticity of an identity card or residence document.**

4.3 Exemptions from fingerprinting

55. Article 3(5)(a) of the Proposal states that children under the age of 12 years and persons where fingerprinting is physically impossible are exempted from the requirement to give fingerprints. **The EDPS welcomes the introduction of exemptions from giving fingerprints based on the age of the person or his/her inability to provide fingerprints**. These exemptions are part of the fallback procedures that should be implemented.

56. At the same time, the EDPS draws attention to the need to consider the **best interest of the child** in all actions public authorities and private actors take concerning children, in line with Article 24 of the Charter. Similarly, Recital 38 of the GDPR states that "*[c]hildren merit specific protection with regard to their personal data, as they may be less aware of*

the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."

57. In this context, the EDPS would like to stress that as regards large populations the age limit for collecting children's fingerprints is currently established at the level of 14 years[50]. Taking into account **the wide range and potential impact of the Proposal** outlined above, the EDPS recomments **setting the age limit for collecting children's fingerprints under the Proposal at 14 years, in line with other instruments of EU law.**

58. Furthermore, we note that the Proposal aims also to **extend the requirements for the fingerprinting of children, to those who hold the residence documents** because of the fact that they are non-EU family members of EU citizens. In line with the EDPS remarks above, **the EDPS recommends to set the age limit in the Proposal at 14 years.**

7. CONCLUSIONS

The EDPS observes that the Commission has clearly chosen to prioritise the free movement aspects of the Proposal and to treat the security-related objective as corollary. The EDPS remarks that this might have an impact on the analysis of necessity and proportionality of the elements of the Proposal.

The EDPS supports the objective of the European Commission to enhance the security standards applicable to identity cards and residence documents, thus contributing to security of the Union as a whole. At the same time, the EDPS considers that the Proposal does not sufficiently justify the need to process two types of biometric data (facial image and fingerprints) in this context, while the stated purposes could be achieved by a less intrusive approach.

Under the EU legal framework, as well as within the framework of Modernised Convention 108, biometric data are considered sensitive data and are subject to special protection. The EDPS stresses that both facial images and fingerprints that would be processed pursuant to the Proposal would clearly fall within this sensitive data category.

Furthermore, the EDPS considers that the Proposal would have a wide-ranging impact on up to 370 million EU citizens, potentially subjecting 85% of EU population to mandatory fingerprinting requirement. This wide scope, combined with the very sensitive data processed (facial images in combination with fingerprints) calls for close scrutiny according to a strict necessity test.

In addition, the EDPS acknowledges that, given the differences between identity cards and passports, the introduction of security features that may be considered appropriate for passports to identity cards cannot be done automatically, but requires a reflection and a thorough analysis.

Moreover, the EDPS wishes to stress that Article 35(10) of the GDPR would be applicable to the processing at hand. In this context, the EDPS observes that the Impact Assessment

accompanying the Proposal does not appear to support the policy option chosen by the Commission, i.e. the mandatory inclusion of both facial images and (two) fingerprints in ID cards (and residence documents). Consequently, the Impact Assessment accompanying the Proposal cannot be considered as sufficient for the purposes of compliance with Article 35(10) GDPR. Therefore, the EDPS recommends to reassess the necessity and the proportionality of the processing of biometric data (facial image in combination with fingerprints) in this context.

Furthermore, the Proposal should explicitly provide for safeguards against Member States establishing national dactyloscopic databases in the context of implementing the Proposal. A provision should be added to the Proposal stating explicitly that the biometric data processed in its context must be deleted immediately after their inclusion on the chip and may not be further processed for purposes other than those explicitly set out in the Proposal.

The EDPS understands that using biometric data might be considered as a legitimate anti-fraud measure, but the Proposal does not justify the need to store two types of biometric data for the purposes foreseen in it. One option to consider could be to limit the biometrics used to one (e.g. facial image only).

Moreover, the EDPS would like to underline that it understands that storing fingerprint images enhances interoperability, but at the same time it increases the amount of biometric data processed and the risk of impersonation in case of a personal data breach. Thus, the EDPS recommends to limit the fingerprint data stored on the documents chip to minutiae or patterns, a subset of the characteristics extracted from the fingerprint image.

Finally, taking into account the wide range and potential impact of the Proposal outlined above, the EDPS recommends setting the age limit for collecting children's fingerprints under the Proposal at 14 years, in line with other instruments of EU law.

Brussels,

(**signed**)

Giovanni BUTTARELLI

Notes

[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), OJ L 119, 4.5.2016, p. 1–88
[2] OJ L 119, 4.5.2016, p. 1.
[3] OJ L 8, 12.1.2001, p. 1.
[4] OJ L 119, 4.5.2016, p. 89.
[5] Proposal for a Regulation of the European Parliament and of the Council of 17 of April 2018 *on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement*, COM(2018) 212 final, 2018/0104 (COD)
[6] Communication from the Commission to the European Parliament and the Council of 8 of December 2016: *Action plan to strengthen the European response to travel document fraud*, COM(2016) 790 final
[7] Communication from the Commission to the European Parliament, the European Council and the Council *Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders,* COM(2016) 602 final.
[8] The Explanatory Memorandum of the Proposal, p. 2
[9] Article 1 of the Proposal
[10] The Impact Assessment that accompanying the Proposal, SWD(2018) 110 final, p. 21
[11] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, OJ L 158, 30.4.2004, p. 77–123
[12] The ICAO Document 9303 (seventh edition, 2015), part 9, chapter 3.1.
[13] Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals, OJ L 157 of 15.6.2002, p. 1.
[14] Article 2 of the Treaty on the European Union *("TEU")* states that *"The Union is based on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities"*. In addition, Article 6(1) TEU recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg on 12 December 2007, which has the same legal value as the treaties, and Article 6(3) TEU states that *"fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law"*.
[15] ECtHR judgment of 13 May 2008, *case S. and Marper v. United Kingdom*, §§ 68 and 84, ECHR 2008
[16] Article 4(14) of the 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), OJ L 119, 4.5.2016, p. 1–88.
[17] See Article 9 of the 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), OJ L 119, 4.5.2016, p. 1–88 and Article 10 of the Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, OJ L 119, 4.5.2016, p. 89–131.
[18] Article 6 of the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data adopted on 17-18 May 2018 by
[19] The General Data Protection Regulation refers to sensitive personal data as *"special categories of personal data"* (see Article 9 of the 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), OJ L 119, 4.5.2016, p. 1–88)
[20] EDPS Toolkit: *Assessing the necessity of measures that limit the fundamental right to the protection of personal data*, 11 April 2017
[21] Recital 6 of the Proposal

[22] Annex 5 to the Impact Assessment accompanying the Proposal, p.104-105. See also Section 2.3 of the CSES report, which contains further information on the types of ID cards and residence documents issued by national authorities.
[23] The Impact Assessment accompanying the Proposal, p.12
[24] Impact Assessment accompanying the Proposal, p.9 and Annex 8 to the Impact Assessment accompanying the Proposal, p.123
[25] Annex 8 to the Impact Assessment accompanying the Proposal, p.123
[26] 16 Member States would be subject to this new obligation: Austria, Croatia, Czech Republic, Finland, France, Greece, Ireland, Italy, Luxembourg, Malta, Netherlands, Poland, Romania, Slovakia, Slovenia and Sweden. See: Annex 8 to the Impact Assessment accompanying the Proposal, p.123
[27] Page 7of the Proposal.
[28] The Impact Assessment accompanying the Proposal, p.4, Although it is not clear from the report, it is assumed that there is significant overlap between those two numbers
[29] Impact Assessment accompanying the Proposal, p.12
[30] Annex 6 to the Impact Assessment accompanying the Proposal, p.109, FRONTEX. 2016. Annual Risk Analysis. p. 14.
[31] FRONTEX Risk Analysis, p.22
[32] Annex 6 to the Impact Assessment accompanying the Proposal, p.109
[33] In this context, it is worth to highlight that even the Commission in the above mentioned Impact Assessment admits that *"the number of documents detected does not seem very high"*. See: Impact Assessment accompanying the Proposal, p.12
[34] 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), OJ L 119, 4.5.2016, p. 1–88
[35] ECJ Judgment of 17 October 2013, Case C‑291/12, *Schwarz v. Stadt Bochum*
[36] The Impact Assessment accompanying the Proposal, p.51
[37] The Impact Assessment accompanying the Proposal, p.27
[38] The Explanatory Memorandum to the Proposal, p.6
[39] enshrined in Article 5(1)(b) of the GDPR
[40] The Action Plan of December 2016, p.10
[41] The Action Plan of December 2016, p.11
[42] The Impact Assessment accompanying the Proposal, p.14
[43] ECJ Judgment of 17 October 2013, Case C‑291/12, *Schwarz v. Stadt Bochum*
[44] ECJ Judgment of 17 October 2013, Case C‑291/12, *Schwarz v. Stadt Bochum*, par 37
[45] The Impact Assessment accompanying the Proposal, p.60
[46] Art 5(1)(c) of the GDPR
[47] Cropped and downsampled finger pattern followed by the cellular representation of the finger pattern image to create the finger-pattern interchange data.
[48] Part 9, chapter 4.2.
[49] Skimming is a type of attack that uses a device near the ID Card to collect the documents data when used.
[50] See for example: Article 14 of the Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 *on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, OJ L 180, 29.6.2013, p. 1–30