APPENDIX

1. Interferences with the fundamental rights to private life and the protection of personal data

In respect of the recently presented Commission documents:

a. the (updated) proposal for the creation of an Entry/Exit system (EES)
b. the Communication on Stronger and Smarter Information Systems for Borders and Security;
c. the Report on the availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II);
d. the Communication on the European Agenda on Security to fight against terrorism; and
e. the proposal to amend the current Eurodac Regulation,

the Article 29 Working Party (WP29) considers that the proposals of the Commission will have an impact on the right to private life and the right to the protection of personal data, as established by Article 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter: the Charter) and Article 8 of the European Convention on Human Rights (hereinafter: the Convention).

On numerous previous occasions, the WP29 has stressed that **new legislative proposals have to be compliant with fundamental rights in general and with the right to private life and the right to the protection of personal data in particular**.[1] In addition, based on Article 52 of the Charter and in accordance with settled case-law of the Court of Justice of the European Union (CJEU), the principles of necessity and proportionality require that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and strictly necessary in order to achieve those objectives.[2] Taking into account this applicable legal framework, the WP29 would like to draw attention to a number of issues relating to the proposals of the Commission that raise concerns from a data protection perspective.

2. Necessity and proportionality of the Entry Exit System (EES) and the Eurodac proposal

The WP29 recalls that it is settled case law that the principle of proportionality requires that measures implemented by acts of the European Union are necessary to achieve the objective pursued.[3] Moreover, derogations and limitations in relation to the protection of personal data must apply only insofar as is strictly necessary.[4]

The EES

Pursuant to Article 1 of the proposal, the EES will consist of a centralised storage system for the recording and storage of information on the date, time and place of entry (or refusal thereof) and exit of third country nationals (TCNs) crossing the external borders of the Member States. The system will generate alerts to Member States when authorised periods for stay have expired and the database may

[1] Such as Opinion WP145 on the use of Passenger Name Record (PNR) for law enforcement purposes, Opinion WP78 on the global approach to transfers of Passenger Name Record (PNR) data to third countries, Opinion WP206 on Smart Borders and Opinion WP211 on the application of necessity and proportionality concepts and data protection within the law enforcement sector.

[2] See, to that effect, Case C‑343/09 Afton Chemical paragraph 45; Volker und Markus Schecke and Eifert paragraph 74; Cases C‑581/10 and C‑629/10; Nelson and Others paragraph 71; Case C‑283/11 Sky Österreich paragraph 50; and Case C‑101/12 Schaible paragraph 29); C-362/14 Max Schrems, paragraph. 92 and C-293/12 Digital Rights Ireland, paragraph. 52.

[3] C-58/08 Vodafone and others, par. 51.

[4] C-73/07, Satakunnan Markkinapörssi and Satamedia, par. 56.

furthermore be used for identification purposes within the territory of the Member States to identify TCNs who do not or no longer fulfil the conditions for entry, stay or residence within the territory of the Member State.[5] In addition, access for law enforcement authorities is envisaged from the outset, under conditions as prescribed in Chapter IV of the proposal.

According to Article 5 of the proposal, the EES serves numerous objectives[6], but - as stated by the Commission - the EES is first of all aimed at improving the management of external borders.[7] Secondly, the EES is aimed at reducing irregular migration by addressing the phenomenon of overstayers and, thirdly, at contributing to the fight against terrorism and serious crime, thereby contributing to ensuring a high level of internal security.[8] In order to achieve these objectives, a combination of alphanumeric (amongst others name and passport number) and biometric data (facial image, four fingerprints) will be stored in the system.

In 2013, the WP29 expressed its concerns regarding the necessity and proportionality of the EES as such in Opinion 05/2013 on Smart Borders.[9] At the time, the WP29 called into question whether the EES would be effective in achieving its aims and - even if it were accepted that the EES would provide significant added value - whether the added value of the EES would meet the threshold of necessity and proportionality.[10]

The WP29 has noted that in the Impact Assessment (IA) accompanying the current proposal for establishing the EES, the necessity of an EES is now assumed, due to the recent refugee crisis and terrorist attacks.[11] In this regard, the WP29 remarks that the primary objective of the EES is improving the management of external borders and is, as such, not directly related to these recent developments.[12] While the secondary objectives are related to the combatting of irregular migration and may provide an additional instrument for law enforcement authorities to prevent and combat terrorism, the WP29 nonetheless advises that the necessity and proportionality of the EES in relation to the primary objectives be substantiated. In this light, and reiterating its earlier Opinion on the EES as expressed in 2013, the WP29 makes the following observations regarding the current proposal for establishing the EES.

Regarding the first objective of the EES, the Commission states that the current system for border management regarding third country nationals is based on stamps in passports and prone to errors and fraud, amongst others because of the unreadability of stamps. This in turn leads to time-consuming procedures at borders. The WP29 however notes that the EES itself also provides for complex processes and that it is therefore not clear whether the EES will - in practice - lead to more efficient

[5] Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 Brussels, 6.4.2016, COM(2016) 194 final, Article 25.
[6] Ibid, Article 5 (a) to (l)
[7] Ibid, Explanatory memorandum, p. 2-3,
[8] Ibid.
[9] Article 29 Working Party Opinion 05/2013 on Smart Borders (WP 206)
[10] Ibid, p. 13.
[11] Impact Assessment Report on the establishment of an EU Entry Exit System accompanying the document "Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011" and "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/xxx as regards the use of the Entry/Exit System (EES)", Brussels, 6.4.2016, SWD(2016) 115 final, p. 2. (hereinafter referred to as: EES Impact Assessment 2016).
[12] EES Impact Assessment 2016, p. 2.

and reliable border controls, in particular taking into account the fact that the EES will include biometric data, which entails a risk of error.[13] In addition, the WP29 recalls its earlier statement that creating a large scale database holding biometric data in order to streamline procedures at border crossings, is not proportional.[14] The effectiveness of the EES regarding the border management system is furthermore fully depending on the quality and accuracy of the inserted data.[15] In conjunction therewith - and taking into account concerns regarding data quality in current information systems[16] - the **WP29 therefore stresses the need to ensure the accuracy and quality of data processed in the EES** *in practice*[17], since inaccurate data or data of a low quality may have far-reaching consequences for individuals such as a wrongful eviction or denial of access.[18]

Regarding the second objective of the EES - reducing irregular migration by addressing the phenomenon of overstaying - the WP29 recalls its earlier statement that creating more insight in the number of overstayers is in itself not a means to carry out the effective return of overstayers.[19] This objective needs to be accompanied by an effective (EU) policy to facilitate the actual return process *in practice*.[20] In this light, the WP29 advises the Commission to investigate whether existing legal and practical avenues regarding the return of irregular migrants are fully and effectively used, before a new large-scale information system is introduced. If the primary objective of the EES is however to gain better insight into the actual amount of overstayers, then the WP29 advises to investigate whether there are less intrusive ways that could lead to this result, such as the use of anonymous statistical data or the information already available in the VIS. In this regard, the WP29 recalls that **the CJEU has specified that it should be demonstrated that the same purpose cannot be achieved with less intrusive means**.[21]

Regarding the third objective, the WP29 recognizes the importance of sufficient information for law enforcement authorities to effectively prevent and combat terrorism and serious crimes.[22] However, the WP29 stresses that several EU information systems - most notably the Schengen Information System II (hereinafter SIS II) - already provide for access for law enforcement authorities, and include

[13] At first entry alphanumeric and biometric data will be enrolled. This data will have to be verified and confirmed by a border guard. Before a new individual file is created, border guards must however first search whether a file already exists. This search in the EES (and possibly into the VIS) will have to be carried out in a de-duplication effort to ensure that the passenger is not already enrolled under the same or another identity. Border guards should also inform the passengers of their remaining authorized stay and of their rights. Not only is the procedure in itself quite complicated, it is also not entirely clear in which cases the VIS will be accessed. See: Diana Dimitrova, "The Smartification of EU Borders", (CiTiP Working Paper Series, KU Leuven, June 2016, p.6-7). This issue was also raised in the Article 29 Working Party Opinion 05/2013 on Smart Borders, p. 5-6.

[14] Article 29 Working Party Opinion 05/2013 on Smart Borders (WP 206), p. 8.

[15] As was also stated in the Article 29 Working Party Opinion 05/2013 on Smart Border (WP 206)s, p. 6.

[16] Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, p. 10.

[17] The right of access, correction and deletion are explicitly laid down in Article 46 of the EES Proposal.

[18] As was also stated in the Article 29 Working Party Opinion 05/2013 on Smart Borders (WP 206), p. 8.

[19] Article 29 Working Party Opinion 05/2013 on Smart Borders (WP 206), p. 8-9.

[20] In this light, the WP29 notes that the EU Return Directive (2008/115/EC) imposes a legal obligation on Member States to issue a return decision to any third-country national who stays irregularly on their territory and – where called for – to take measures to enforce it. The Commission is currently evaluating the state of the application of the Directive. In the EU Action Plan on return (Brussels, 9.9.2015, COM(2015) 453 final), it is noted that less than 40% of the irregular migrants that were ordered to leave the EU departed effectively. While these statistics apply to all irregular migrants and not to the phenomenon of overstayers as such, these statistics provide a clear indication that the current return policy shows deficiencies in practice.

[21] C-92/09 Volker und Markus Schecke GbR v. Land Hessen and C-93-09 Eifert v. Land Hessen and Bündesanstalt für Landwirtschaft und Ernährung.

[22] It is apparent from the case-law of the Court of Justice that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C‑402/05 P and C‑415/05 P Kadi and Al Barakaat International Foundation v Council and Commission and Cases C‑539/10 P and C‑550/10 P Al-Aqsa v Council). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C‑145/09 Tsakouridis).

information on third country nationals. Further recommendations on this issue can be found under paragraph 4 of this appendix.

Based on the observations above and taking into account Article 7 and 8 jo. 52 of the Charter, the WP29 advises to further substantiate the **necessity and proportionality of the proposal to create an EES in order to achieve the objectives as mentioned by the Commission**. Specific recommendations regarding the access for law enforcement authorities, the use of biometric data and data retention can be found in paragraphs 4, 5 and 6.

Eurodac

In the new Eurodac proposal the scope of the system is expanded from determining which EU country is responsible for the processing of an asylum application in line with the Dublin regulation, to identifying illegally staying third-country nationals and those who have entered the EU irregularly in order to assist Member States to re-document third-country nationals for return purposes. In practice, this means that in addition to personal data of asylum seekers, personal data of third-country nationals and stateless persons who have entered the EU irregularly or are found illegally on the territory of a Member State will be collected and processed for this new purpose.

Since personal data (both alphanumeric data and biometric data, consisting of facial recognition and ten fingerprints) will be collected, stored and processed based on the proposed extension of the scope of Eurodac and the extension of the data collection, the proposal can be considered to be an interference with the fundamental rights to privacy and data protection as laid down in Articles 7 and 8 of the Charter. Based on article 52 of the Charter and jurisprudence of the CJEU, this means that the proposal needs to be strictly necessary and proportional. In this light, the **WP29 expresses its concerns regarding the lack of any privacy and data protection impact assessments of the extension of the scope, data collection and purposes of Eurodac and advises the Commission to initiate such an assessment.** Such an assessment is a necessary tool to assess the proportionality of a new measure introduce by the legislator and which could have an impact on the privacy and the personal data of individuals.

Furthermore, the WP29 notes that the proposal to extend the scope of Eurodac allows for the transfer to third countries of personal data of asylum seekers, third country nationals and stateless persons for the purpose of return and readmission.[23] These transfers may however have profound consequences for individuals, especially for those who have fled their country of origin out of fear of persecution. In this respect, and in accordance with the principles of *data minimisation* and *proportionality*, the WP29 recommends specifying in the Proposal that only the data necessary for the purpose of return or repatriation can be transferred to the third country.

Regarding the **international transfer of data to public or private entities outside of the EU**, the WP29 recommends clarifying under which circumstances such a transfer can take place, since the general framework on data protection[24] already provides for strict rules concerning the international

[23] Proposal for a Regulation of the European parliament and of the Council 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] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, Brussels, 4.5.2016, COM(2016) 272, Article 38.

[24] Article 37(4) of the Proposal refers to the General Data Protection Regulation: "in accordance with Chapter V of Regulation 2016/679" as mentioned in Article 37(4)".

transfer of data to third countries. Therefore, the interaction between the Eurodac regulation and these instruments should be clarified, by example through mentioning whether the rules provided under Article 37 are to be applied in addition to the rules on international transfer under Chapter V of the General Data Protection Regulation (GDPR)[25], respectively the rules on international transfer under Chapter V of the Directive[26] for the police and criminal justice sector.[27]

Lastly, the WP29 notices that the new Eurodac-proposal allows for the use of real personal data by EU-Lisa when testing the Central System for diagnostics and repair as well as for the use of new technologies and techniques. The WP29 emphasizes that, following the necessity principle, in principle "dummy data" should be used when testing new systems or technologies. Only when a legitimate objective - in practice - cannot be achieved by using dummy data, real personal data may be used. The Explanatory Memorandum states that the use of dummy data by EU-Lisa has failed to yield good test results in practice.[28] It is however not clear for the WP29 how the use of real data can give better results in this respect. In addition, the objectives for which real personal data may be used according to the new Eurodac proposal are broad, especially the use of personal data for testing "new technologies and techniques". **The WP29 therefore advises to introduce clear categories and restrictions regarding the use of real personal data for testing purposes, in order to make sure that no more personal data is processed than strictly necessary in the context of testing purposes**. In conjunction to this, the WP29 would like to recall that any data allowing to identify an individual directly or indirectly are to be considered personal data.[29] Therefore, since biometric data by nature allow such identification, this category of data cannot be considered as data anonymised (for testing purposes), contrary to what is implied under Article 5 (2), last paragraph [30]. The WP29 therefore advises to clarify this particular wording.

---

[25] Respectively Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995on the protection of individuals with regard to the processing of personal data and on the free movement of such data, if this Directive is still applicable when the new Eurodac proposal enters into force.

[26] 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

[27] Respectively Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, if this Framework Decision is still applicable when the new Eurodac proposal enters into force.

[28] Proposal for a Regulation of the European parliament and of the Council 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] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, Brussels, 4.5.2016, COM(2016) 272, final Explanatory Memorandum, p. 16

[29] Article 29 Working Party Opinion 4/2007 on the concept of personal data (WP 136), Article 4 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 3 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

[30] Article 5 (2): Eu-LISA shall be permitted to use real personal data of the Eurodac production system for testing purposes in the following circumstances:
(a) for diagnostics and repair when faults are discovered with the Central System; and
(b) for testing new technologies and techniques relevant to enhance the performance of the Central System or transmission of data to it.
In such cases, the security measures, access control and logging activities at the testing environment shall be equal to the ones for the Eurodac production system. *Real personal data adopted for testing shall be rendered anonymous in such a way that the data-subject is no longer identifiable*.

In light of the observations above, the **WP29 advises the Commission to carry out a privacy and data protection impact assessment of the extension of the scope and purposes of Eurodac**. Specific recommendations regarding the access for law enforcement authorities, the use of biometric data - including biometric data of children - and data retention can be found in paragraphs 4, 5 and 6.

3. Interoperability of systems

The WP29 notes that the process towards the interoperability of information systems at EU level - which may result in a common repository of data including the VIS, SIS, EURODAC and the new EES[31] - raises fundamental questions regarding the purpose, necessity and proportionality of the data processing involved. Since the different options are still being consulted on, the WP29 would like to contribute to the debate by making some general observations.

First of all, the WP29 stresses the need to make full and effective use of the existing legal avenues in the current EU large-scale information systems, before any new system or the interoperability of systems should be discussed. [32] **Only when existing information systems have proven to be insufficient, it will be possible to substantiate the actual necessity and proportionality of the interoperability of systems**, as required according to Articles 7 and 8 jo. 52 of the Charter. The WP29 therefore advises the Commission to examine if current legal instruments are fully used before the interoperability of systems will be envisaged.

Secondly, different information systems co-exist as they serve different purposes. By striving for the interoperability of systems - possibly resulting in the combining of individual data elements stored in different information systems in one common repository - there is a risk that the principle of purpose limitation as enshrined in Article 7 of the Charter will be nullified. The WP29 therefore recommends to specifically focus on the principle of purpose limitation when developing a new strategy for the EU's information systems. In addition, the WP29 notes that merging personal data from different information systems into one common repository will - in all likelihood - not lead to data minimisation[33], but may rather impair this principle. Creating a common repository may avoid a situation where the same data is stored simultaneously on different systems as the Commission notes. **The WP29 is however concerned that placing personal data from separate systems in one common repository, with access for different purposes and by different authorities, may rather enhance, than minimise, the large scale processing of personal data**. Moreover, a common repository of data may result in a discriminatory situation, since it will – in all likelihood – mainly hold personal data from *third country nationals*, most of whom are not suspected of illegal activities.

[31] The interoperability of information systems means "the ability of information systems to exchange data and to enable the sharing of information". In its pursuit of the interoperability of information systems, the Commission distinguishes different dimensions of interoperability, varying from a single search interface to query different information systems simultaneously, to the interconnectivity of information systems (as is proposed for the EES and VIS) and the establishment of a shared biometric matching service, eventually resulting in a common repository of data for different information systems ("core module"). This common repository of data is the most ambitious approach to interoperability and would constitute "a core module that contains basic data (alphanumeric and biometric), while other data elements and specific features of the different information systems (e.g. visa data) would be stored in different modules". The core module and the specific modules would then be connected to link the respective data sets so that, "when necessary, the common repository would allow for the recognition of connections and provide an overall picture by combining individual data elements stored in different information systems". See: Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, p. 14.

[32] In this regard it is important to note that "a general concern in relation to information systems is the level of implementation by Members States". See: Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, p. 10.

[33] See: Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, p 18.

The WP29 therefore recommends to take note of these risks when consulting the possibilities regarding the interoperability of systems.

The WP29 furthermore notes that allowing access for different purposes and by different authorities in one common repository may weaken one of the core principles of data protection, namely the possibility to clearly define the controller responsible for the processing of particular data. In conjunction therewith, the possible "mixing" of purposes and access rights of different authorities in a common repository, may also hinder the monitoring of the lawfulness of data processing by the data protection authorities and may lead to a lack of clarity concerning the appropriate data retention periods, which are defined differently in each system.

In light of the interests at stake, and while fully aware that the process towards the interoperability of information systems at EU level is still being consulted on, the **WP29 emphasizes the need to adhere to the principles of purpose limitation, data minimisation, data retention and clear identification of a data controller, when developing new proposals** in line with Article 7 and 8 jo. 52 of the Charter.

4. Access for law enforcement purposes

The WP29 would like to recall that persons whose data are or will be stored in VIS, Eurodac and EES are in principle not suspected of any crimes and should subsequently not be treated as such, since these systems are designated mainly for different purposes. The WP29 therefore expresses its concerns regarding the proposal for the modification of the Schengen Borders Code[34], which envisages an obligation to carry out systematic checks against relevant law enforcement databases at the external border on all persons, including EU citizens, in order to screen individuals who may pose a threat to public order and internal security.

The WP29 stresses that **the necessity of law enforcement access should be based on solid evidence which can justify such intrusion in the privacy of individuals**. Consequently, access to these databases by law enforcement authorities should be introduced only after evaluation of the existing systems and should not be introduced into new systems by default**.** In addition, the WP29 notes that there are strong indications that existing information systems with access for law enforcement authorities are not put into full and effective use at the moment.[35] In light of this, it is worth mentioning that no evaluation of the necessity and effectiveness of access by law enforcement authorities to VIS and Eurodac has taken place and that solid evidence of the usefulness of this access seems to be lacking. The same concerns apply to access by Europol to existing databases. At the moment, Europol has the mandate to access data when necessary for performance of its tasks, but is not directly connected to Eurodac and VIS databases. In addition, the number of searches done by Europol in SIS II is very limited as is stated in the Communication on Stronger and Smarter Information Systems for Borders and Security.[36] Despite this, the Commission proposes, in the same Communication, to provide further access by other EU Agencies. Therefore, **the WP29 regrets that the access by law enforcement authorities and Europol to the EES is granted ex ante and not ex**

[34] Proposal for a regulation of the European Parliament and of the Council amending Regulation No 562/2006 (EC) as regards the reinforcement of checks against relevant databases at external borders, COM(2015) 670 final.
[35] Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final, p. 10.
[36] Communication from the Commission to the European Parliament and the Council Stronger and Smarter Information Systems for Borders and Security, COM(2016) 205 final

post evaluation, as was initially planned in the first Smart Borders proposal. This approach may lead to an unnecessary interference with the right to privacy.

The WP29 welcomes the efforts made in the Eurodac and EES proposal to give the responsibility of verifying the access request of the law enforcement authorities to a "verifying authority". However, since this authority is supposed to be part of the same organisation as the designated authority that requested access, the independence of such a verifying authority cannot be guaranteed. Therefore, **the WP29 recommends obliging the verifying authority to be actually independent from the designated authority**.

Concerning the Eurodac proposal - the WP29 regrets that a difference is made regarding the period for which access for law enforcement purposes to Eurodac data is allowed regarding individuals who were granted international protection[37], and other individuals. Access for law enforcement purposes will only be possible for a period of three years for the first category of individuals, while this restriction does not exist for the other category. Since the WP29 has not been able to distinguish a clear justification for this different treatment, it recommends to either clarify or reconsider this decision.

Finally, the WP29 recommends clarifying what is meant by "marking of data" since the Eurodac Proposal does not define this term. **A clear description of the marking that will be performed on the data of the individuals should be included in the Proposal**. This is even more relevant due to the fact that the marking of individuals under Article 19(4) is a new marking, which seems different from the marking for law enforcement purposes provided under Article 19 (1) and (2).

5. Use of biometric data

The WP29 notes that the Commission proposes to add a new biometric identifier - facial recognition - into VIS, Eurodac and EES, which will supplement the personal data already available in those systems, namely dactyloscopic data (VIS and Eurodac – 10 fingerprints, EES – 4 fingerprints) and a wide range of alphanumeric data. At the same time, the Commission proposes to launch the automated fingerprints search functionality in SIS II by mid-2017, which is inevitably related with the need to introduce the right of data subjects to object to automated processing,[38] and to add in the future facial recognition as additional biometric identifier.

The WP29 would like to recall that the use of biometric data is inseparably connected with the proportionality and necessity principles. As it was previously said in the Opinion on development in biometrics technologies[39], **biometrics may be processed only if this is adequate, relevant and not excessive and if the purpose for processing cannot be achieved in a less intrusive way**. The WP29 notes that an infringement of the right to privacy of any individual must be proportional to any anticipated benefit. In addition, the WP29 would like to emphasize that, following the adoption of the

[37] Proposal for a Regulation of the European parliament and of the Council 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] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, Brussels, 4.5.2016, COM(2016) 272, final, Article 19 (2).

[38] Communication from the Commission to the European Parliament, the European Council and the Council delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union (COM(2016) 230 final)

[39] Article 29 Working Party Opinion 3/2012 on development in biometrics technologies (WP 193)

General Data Protection Regulation[40] and Police and Justice Data Protection Directive[41], all kinds of biometric data will, from 25 May 2018, be treated as special category of personal data and in consequence should be processed only in exceptional situations defined by law. The WP29 moreover notes that the public consultation on Smart Borders has shown that the public itself is "mainly concerned with the perceived intrusiveness of biometrics, the proportionality of the measures, the risks of a potential data misuse or theft."[42] The WP29 therefore stresses that **the need to collect additional data, and especially biometric data which are sensitive data, should be demonstrated by a prior analysis**.

In this light, and as already noted in the 2013 Opinion on Smart Borders[43], the WP29 considers that biometric data should only be introduced after an evaluation of the system after some years of operation. Such an evaluation should provide a factual basis of whether the objectives could be achieved without processing biometrics. Therefore the WP29 advises the **Commission to present clear evidence to prove the necessity of adding a supplementary biometric identifier**, taking into account that the large scale IT systems currently used for border management, visa policy and asylum procedures already contain catalogues of data sufficient to achieve the objective of identifying persons. Arguments of convenience, cost and time effectiveness cannot justify what the WP29 considers as a serious interference in fundamental rights.

The WP29 also expresses serious **reservations regarding the proposals of reducing the age limit for collecting fingerprints of children** to the age of 6 years in Eurodac and VIS, which may constitute a particularly intrusive infringement of the privacy of minors, who should be treated with special care. In this regard the WP29 would like to recall recital 38 of the General Data Protection Regulation, which states that "children 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." The WP29 is of the opinion that detailed explanation and specific guarantees regarding the notion of "taking fingerprints and facial images of minors from the age of six (…) in a child-friendly and child-sensitive manner"[44] are needed.

Furthermore, the WP29 notes that according to Article 46 of the proposal for establishing the EES and Article 31 of the Eurodac proposal, data subjects who want to exercise their right to access, correction or erasure, need to submit all personal data, including fingerprints when submitting a request. The WP29 is of the opinion that this requirement may constitute a substantial obstacle to the effective

[40] Article 9 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

[41] Article 10 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

[42] Report on the public consultation on Smart Border, available at http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/docs/consultation_030/results_of_the_public_consultation_on_smart_borders_en.pdf, p. 2

[43] Article 29 Working Party Opinion 05/2013 on Smart Borders (WP 206)

[44] Art. 2 (2) Proposal for a regulation of the European Parliament and of the Council 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] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) 272 final Article 2(2) refers to a "child-friendly and child sensitive" manner to take the facial images of the children, but without specifying what is meant by these terms. A reference is also made the preservation of the dignity and the physical integrity of the children, as if this as not valid for adults.

exercise of the data subject's rights to data protection. As it was previously said in the Opinion on development in biometrics technologies[45], biometrics may be processed only if this is adequate, relevant and not excessive and if the purpose for processing cannot be achieved in a less intrusive way. Data subjects therefore should – as a principle – only be required to supply alphanumeric data when submitting a request. The use of biometric data should be restricted to special circumstances, for instance in case of a mismatch or a homonym in the system when processing a request.

Lastly, the WP29 notes that the Eurodac recast Proposal provides that Member States can impose administrative sanctions for non-compliance with the fingerprinting process**.** The WP29 shares the views of the Eurodac Coordinated Supervision Group which stated that "As the purpose of Eurodac is not to add the criterion 'having readable fingerprints' to the list of criteria for being granted asylum, but to detect and prevent multiple applications, the fact that a person has illegible fingerprints should not be used against him/her. In fact, this would be discriminating behaviour"[46].

6. Retention periods and categorisation of data

In accordance to the European legal framework regarding the protection of personal data[47], personal data should be retained only for as long as necessary to achieve a legitimate purpose. It is also important to recall the judgement of the CJEU in the case Digital Rights Ireland Ltd[48] in which it was said that "the determination of period of retention must be based on objective criteria in order to ensure that it is limited to what it is strictly necessary".

The WP29 notes that the data retention period in the EES has been extended from 181 days - as was the case in the 2013 proposal - to five years in the current proposal for the introduction of an EES. **Taking into account the declared purposes, the WP29 holds strong doubts regarding the proportionality of the proposal to extend the data retention period in the EES beyond the validity of visa**. In this regard, it is worth mentioning that the results of the public consultations on Smart Borders launched by the Commission in 2015 also show that the majority of those surveyed were opposed to the extension of the data retention period.[49]

Varied retention periods could be introduced for persons who legally stay on EU territory as well as for overstayers, but the WP29 underlines that such a differentiation should also be proportionate and necessary. In this respect, the WP29 notes that the blanket retention period of five years for overstayers in the EES is not appropriately justified, and therefore appears to be arbitrarily determined, and thus disproportionate. In the opinion of the WP29, the retention period for overstayers should be in tantamount to the period of an entry ban in SIS II. And, while the maximum period of an entry ban is five years, each case should be treated individually; when the entry ban is valid for a shorter period, this shorter period should be followed in the EES. Therefore **the WP29 recommends that the retention period should be either justified with reference to an objective criterion or changed to a retention period relating to an objective criterion**.

---

[45] Article 29 Working Party Opinion 3/2012 on development in biometrics technologies (WP 193)

[46] Eurodac Supervision Coordination Group, Report on the coordinated inspection on unreadable fingerprints, May 2013, available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/13-06-10_Report_unreadable_fingerprints_EN.pdf . The Report of the Coordinated Group also stated that "The procedures should clarify that unreadable fingerprints as such are not to be used against applicants, but that any adverse consequences for applicants need to be justified by sufficient evidence."

[47] Directive 95/46/EC, the General Data Protection Regulation and the Police and Justice Data Protection Directive

[48] CJEU, Digital Rights Ireland Ltd (C-293/12), consideration 64

[49] Report on the public consultation on Smart Border, available at http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/docs/consultation_030/results_of_the_public_consultation_on_smart_borders_en.pdf, p. 7

With regard to the Eurodac proposal, **the WP29 also considers that a retention period of five years for all data** (except in case of further erasure when an individual has been granted the nationality of a Member State) **is not justified by the Commission**. The mere reference to the retention period of other instruments[50] cannot be seen as a sufficient justification since these other instruments have other purposes and are used in different circumstances. Moreover, the starting point of the retention period is also an issue, since the Regulation does not define what this starting point is. It seems that the retention period will be prolonged each time that a competent authority will collect the data of an individual, which could lead to an undermined period of conservation of the data. The WP29 therefore recommends to provide in the text that the retention period starts at the first collection of data of the individual.

Lastly, the WP29 notes that the **new Police and Justice Data Protection Directive will require that the data shall be categorised correctly depending on the status of the individual**: victim, witness, suspect etc. In this light the WP29 stresses the need to follow this reasoning in all legislative proposals concerning personal data processing.

[50] As explained in the Explanatory Memorandum to the Proposal for a regulation of the European Parliament and of the Council 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], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM(2016) 272 final , p. 6.