Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the Council and the European Parliament on "Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking"

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 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to Regulation (EC) No 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[2], and in particular Article 28(2) thereof,

Having regard to Council 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[3],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 21 October 2013, the Commission adopted the Communication to the Council and the European Parliament on "Firearms and the internal security of the EU: protecting citizens and disrupting illegal trafficking" (hereafter 'the Communication')[4]. The EDPS welcomes the fact that he was consulted on this Communication prior to its adoption and that he was given the possibility to provide informal comments to the Commission.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] OJ L 350, 30.12.2008, p. 60.
[4] COM (2013) 716 final.

1.2. Objective and scope of the Communication

2. The Communication establishes the strategy of the EU to tackle illegal firearms trafficking. To that extent, it proposes an integrated policy focusing on four priorities:
   - safeguarding the licit market for civilian firearms;
   - reducing diversion of firearms into criminal hands;
   - increasing pressure on the criminal markets;
   - building better intelligence.

3. To achieve these priorities, different tasks are envisaged some of which may involve the processing of personal data and, therefore, impact the right of individuals to data protection:
   - the establishment of an EU standard on marking: personal data could be part of the data marked on the firearm;
   - a simplification of the rules for firearms licensing and the eventuality to require medical and criminal checks as a condition for the lawful purchase and ownership of any firearm. Medical checks imply processing of health data on individuals. Health data is sensitive data in the meaning of Article 8 of Directive 95/46/EC, which requires specific protection[5], and is therefore subject to even stricter data protection requirements. Criminal checks imply the processing of data relating to offences, criminal convictions or security measures and access to criminal records, which may be carried out only under the control of an official authority (as set forth in Article 8(5) of Directive 95/46/EC). the compulsory registration and screening of brokers: the creation of a new database including the processing of brokers' personal data shall respect data protection key principles including justification of the necessity of its creation and the proportionality of the processing as well as its intrusion into privacy;
   - the exploration of technological solutions, such as biometric sensors where personal data is stored in the firearm to prevent use by other people than the owner. The processing of biometric data is subject to strict data protection safeguards and security requirements that will be explained in this Opinion;
   - the promotion of cross-border cooperation to stop illegal possession and circulation of firearms through, amongst others, coordinated collection and sharing of information on firearms crime involving police, border guards and custom authorities. Access to police and customs databases is strictly regulated as will be recalled below;
   - the traceability of firearms used by criminals to identify them and those who acquired the firearm. This measure, if it involves the processing of personal data, will have to provide for specific data protection safeguards;
   - the gathering of more accurate and comprehensive data on firearms-related crime by using jointly existing IT tools such as the Schengen Information System II, the Customs Information System, Europol information sharing tools and iArms, Interpol's tool. As mentioned above, access to existing police and customs database is subject to strict data protection rules.

[5] See Court of Justice cases C-62/90 of 8 April 1992, *Commission/Allemagne*, para. 23, and C-404/92 of 5 October 1994, *X/ Commission*, para 17; ECHR 17 July 2008, *I v Finland* (appl. No 20511/03), paragraph 38 and ECHR 25 November 2008, *Armonas v Lithuania* (appl. No 36919/02), paragraph 40.

4. Data protection therefore appears as one of the core issues deriving from this Communication.

1.3. Objective and scope of the Opinion

5. In view of the Commission's intention to present legislative proposals in 2015, the EDPS will, in this Opinion, highlight and explain the data protection implications of the measures envisaged in the Communication. In doing so, the EDPS wishes to ensure that data protection aspects are duly taken into account in future legislative proposals in this area. To this end, he will recall the applicable EU data protection legal framework, give indications on when its consideration is most relevant, and specify the consequences of the required compliance, measure by measure.

2. GENERAL REMARKS

2.1. The applicable European data protection framework

2.1.1. The protections enshrined in Articles 7 and 8 of the Charter

6. As explained above, some of the priorities and tasks set out in the Commission's Communication, will require new processing operations to be put in place and/or existing processing operations to be modified. The sharing of personal data, including sensitive data, will be encouraged.

7. Such collection of personal data will therefore interfere with the right to respect for private life and to the protection of one's personal data as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (hereinafter: "the Charter"). Article 7 of the Charter, which is similar to Article 8 of the European Convention on Human Rights (ECHR)[6], provides for a general right to respect for private and family life, and protects the individual against interference by public authorities. Article 8 of the Charter gives the individual the right that his or her personal data may only be processed if certain essential requirements are fulfilled. These essential requirements are laid down in Article 8 (2) and (3) of the Charter:
   - personal data must be processed fairly and lawfully, for specified purposes,
   - transparency must be ensured, by giving the data subject rights to access and rectify data concerning him or her,
   - compliance with the rules must be subject to control by an independent authority.

8. Whilst Article 7 protects the individual against interference by the EU and by Member States where they are implementing Union law, Article 8 entitles the individual to *ex ante* protection according to certain standards whenever and by whomever his or her data are processed. The two approaches are different and complementary.

9. In this respect, the EDPS welcomes that it is mentioned, in conclusion of the Communication, that the tasks envisaged will be carried out in respect of the

[6] Council of Europe, ETS No 5, 4.11.1950.

fundamental rights and freedoms enshrined in the Charter, including the rights to privacy and to the protection of personal data.

2.1.2. The data protection law applicable to the measures proposed by the Commission concerning firearms

10. It is essential that an explicit reference is made to the applicable EU data protection law in all future EU legislations that will be put forward following the Communication, whenever they contain measures involving the processing of personal data. The EDPS advises that such reference is inserted in a substantive provision of these proposals.

11. Most of the proposals to be put forward further to this Communication would involve the processing of personal data by police and customs authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences. Whenever such processing takes place in the context of the cooperation between authorities of several Member States, Council Framework Decision 2008/977 /JHA applies. When the processing is carried out at national level only, the national data protection rules apply. They may be derived from Directive No 95/46/EC if the Member State has applied data protection rules to criminal matters, or they would otherwise be derived from the principles set forth in the Council of Europe Convention No 108/1981[7].

12. Furthermore, if European databases are created for which EU institutions and bodies will be carrying out part or whole of the processing (e.g. the brokers' database), the rules set forth in Regulation (EC) No 45/2001 will also apply.

2.2. The necessary timely consideration of data protection key principles

13. Data protection requirements must be considered, where possible, at an early stage of the legislative process.

14. The EDPS understands that the aim of this Communication is not to address in detail specific issues. However, as already mentioned, since this Communication proposes measures that will entail the creation of new personal data processing operations or the modification of existing ones, it would be helpful that it raises awareness to the data protection considerations at stake. This would help ensuring that these issues are discussed sufficiently in advance so that, in turn, the measures to be adopted following the communication comply with data protection law.

15. The stakeholders'consultation, that the Commission intends to carry out before presenting its legislative proposals in 2015, is another good opportunity to put key data protection principles in practice. The EDPS recommends that for instance the following issues are discussed: the necessity of the processing, the categories of data necessary to achieve the purposes pursued, the determination of the relevant persons with "a need to know" who may access to data. Professionals involved in fighting firearms trafficking on a daily basis are, indeed, the best positioned to

[7] Council of Europe, ETS No 108/1981, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.01.1981.

determine, with certainty, which data is considered necessary and which seems useless to the achievement of their aim. The EDPS also recommends consulting the European Firearms Expert group on such data protection issues.

16. The EDPS is available to give advice, in particular during these stakeholder consultations. In this perspective, he welcomes that his consultation is foreseen on the gathering of more accurate and comprehensive data on firearms-related crime in the EU and globally[8].

17. Besides, he recalls that he must be consulted on every legislative act that will be drafted pursuant to this Communication as soon as it involves the processing of personal data, pursuant to Article 28(2) of Regulation (EC) No 45/2001.

18. Moreover, for each legislative proposal envisaged, the impact of the proposed measures on the right to the protection of personal data should be measured on the basis of a specific data protection impact assessment. The results of this data protection impact assessment will help defining the data protection requirements that must be specified in each proposal, where necessary.

2.3. The necessary specification of these data protection requirements in future legislations

19. When, pursuant to this Communication, the Commission is to propose legislation involving the processing of personal data, it will have to respect data protection requirements and specify data protection safeguards, with due account of the applicable data protection law for that proposal. More precisely:

- For any situation in which personal data processing is envisaged, the EDPS recommends assessing in the impact assessment the necessity and the proportionality of the processing taking into account the interference with the individual's right to respect for private life and the requirements for the protection of personal data. For instance, before the creation of a new database is considered, it must be assessed whether an existing tool or a less intrusive means would not fulfil the purpose pursued, whether personal data are necessary or anonymised data would be sufficient. If there are plans to have a database accessible to the public, it must be considered whether a less intrusive mean could achieve the same purpose.

- Further to this assessment, pursuant to the purpose limitation principle, the purpose for which data is collected, must be specified in the legislation and if necessary further defined. Attention must be given to the fact that the data collected for one purpose should not be used for any incompatible purposes, without appropriate legal authority. For instance, in the context of fighting against firearms trafficking, if a database of brokers is set up to fight against illegal brokering, this concept should be clearly defined, and the database should not be used for other purposes. For instance, it would not be acceptable to use it to ensure fair competition between brokers.

[8] See Communication page 17, priority 4, task 1.

- Concrete safeguards should be inserted in the legislation to ensure the respect of data protection principles. For instance, the list of the data to be collected should be specified as much as possible, bearing in mind that only data strictly necessary to achieve the purpose pursued should be collected (data minimisation principle). In this perspective, if the creation of a database of firearms brokers is decided as the most relevant tool to achieve the purpose of fighting against illegal brokering of firearms, only the data necessary to identify those brokers should be stored in the database. Data relating to their health history or to the religion or even ethnic origin is not necessary to achieve such purpose. Consequently, this data must not be processed in the database.

- As already mentioned, when sensitive data processing is envisaged, stricter safeguards apply. For instance, if the processing of health data is foreseen in the framework of firearms licensing, access to this data must be restricted to a health professional subject to professional secrecy.

- Data should not be stored for longer than is necessary to achieve the purpose defined: therefore, retention periods should be set up and the choice for a given length of retention should be justified. To follow up on the example of a brokers' database, the future legislation will have to specify the retention period needed to achieve the purpose pursued. It could, for instance, state that data will be kept for the time the individual is working as a broker and up to X years after he does not work as a broker anymore.

- The authority/body responsible for the data processing -the "controller"- should be identified. This controller will, as a result, be in charge of updating the data and ensuring its security. In the brokers' database example, this would translate into the identification of the authority/body responsible for the management of the database and its security. This authority/body would also be the contact point for data subjects exercising their rights.

- Substantive provisions should be inserted to define the modalities according to which the rights of the data subject (in particular, access, modification, and deletion) will be exercised. In our example, this would mean inserting a specific provision stating that the broker whose data is processed has a right to access, modify and delete -under specific circumstances- the data that is processed about him. The provision should specify the contact point and give its contact details or ensure that those are accessible easily to the broker.

- Access to data processed should be limited to those persons of the authority/body having a "need to know". As regards the brokers' database, the future legislation should specify that only authorised officers have access to the data.

- Physical and logical security of the data processed should be ensured.

2.4. The implementation of international instruments at EU level

20. The EDPS notes that the implementation of the Arms Trade Treaty (hereinafter "ATT") and of the United Nation's International Small Arms Control Standards (hereinafter "the ISACS") and the building on the International Tracing Instrument[9] are foreseen in the Communication.

21. These instruments encourage the processing of personal data such as, for example, registers of firearms brokers and national records of export authorizations for the ATT and centralized collection and analysis of data on recovered illicit small arms and light weapons useful to trace those for the ISACS.

22. The EDPS insists that the implementation of these international instruments at EU level should comply with EU data protection legislation, where relevant.

3. SPECIFIC COMMENTS

3.1. The future establishment of an EU standard on marking

23. The Commission intends to investigate the feasibility of an EU marking standard for all weapons (Priority 1, task 2). The EDPS notes that the common marking standard will consist in impressing or engraving a common marking on firearms, which will enable recognition and traceability. He notes that footnote 40, which specifies which elements are included in markings, depending on the manufacturer's choice and national legal requirements, does not refer to personal details of the owner but mentions the manufacturer.

24. The EDPS advises the Commission to specify in the relevant legislative proposal if any personal details, and if so, whose personal details will be processed under this marking. This is of particular importance since no further specification is given regarding personal data to be collected and stored following this marking procedure and since the International Tracing Instrument to which this initiative refers does not list any.

3.2. Firearms licensing and the processing of health and criminal data

25. As mentioned above, the timely consideration of data protection requirements and their specification in the future legislation is of particular importance with regard to some of the processing envisaged in the Communication, which involve the collection of sensitive data.

26. The Commission intends to evaluate the benefits of requiring medical checks as well as criminal records checks as a condition for the lawful purchase and ownership of any firearm[10].

27. The EDPS wishes to draw the Commission's attention to the fact that health data and data on ethnic origin (as mentioned in Priority 3) are considered sensitive data

[9] International instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons, adopted by the United Nations General Assembly on 8 December 2005.
[10] See page 12, task 3, second paragraph of the Communication.

(Article 6 of the Council Framework Decision 2008/977/JHA and Article 8 of Directive No 95/46/EC) and are, as such, subject to strict processing conditions. Furthermore, the processing of criminal data is restricted to competent official authorities, and may in exceptional cases be carried out by a third party only if it is acting under their control (as set forth in Article 8(5) of Directive No 95/46/EC). The EDPS recommends taking these specific conditions into account when drafting legislation on firearms licensing. In any case, the processing of health, ethnic and criminal data should be foreseen by law and meet the requirements of Article 6 of Council Framework Decision 2008/977/JHA and Article 8 of Directive No 95/46/EC.

28. The EDPS therefore insists on the necessity to ensure that data protection safeguards are concretely applied to this specific area and that such safeguards are clearly laid down in the future legislation. In particular, if the project is confirmed, the proposed legislation should specify strictly the purpose of the processing and the restriction of access to data only to the relevant persons who need to know and who are subject to professional secrecy obligations.

29. In addition, the EDPS suggests that the legislative proposal should contain the following elements:
    - A definition should be given of "medical checks" and "criminal records checks". The data that can be processed for these purposes should be strictly listed and procedures to carry out checks should be clearly specified.
    - The medical/criminal grounds for refusing a license should be clearly stated.
    - It should be ensured that no decisions are taken without human intervention and that data subjects' rights (as developed above) are respected.
    - Medical checks and resulting certification should be only carried out and issued by a health professional. Only authorised official authorities should carry out criminal record checks.

3.3. The compulsory registration and screening of firearms brokers[11]

30. The EDPS recommends that the necessity and proportionality of this measure be sufficiently established before putting it into place. He also advises that a data protection impact assessment be carried out, on the basis of which adequate safeguards should be inserted in the future legislation.

3.4. "Smart guns": the possible use of biometric sensors

31. The EDPS notes that the Commission will "explore technological solutions, such as biometric sensors, where personal data is stored in the firearm, for ensuring that purchased firearms may only be used by their legal owner."[12] Such a technology could be obligatory for firearms lawfully sold in the EU to prevent unlawful use due to theft and loss.

32. Biometric data, by their very nature, relate directly to an individual and therefore constitute personal data. A prerequisite to using biometrics is a clear definition of

[11] See Priority 1, task 3, page 12.
[12] See Priority 2, task 2, page 14.

the purpose for which the biometric data are collected and processed, taking into account the risks for the protection of fundamental rights and freedoms of individuals. In its opinion on developments in biometric technologies[13], the Article 29 Working Party insisted that "*the use of biometrics for general security requirements of property or individuals cannot be regarded as legitimate interest overriding the interests or fundamental rights and freedoms of the data subject. On the other hand, biometric data such as fingerprint and/or iris scan could be used for the security of a high-risk area such as a laboratory doing research on dangerous viruses, provided that the controller has demonstrated concrete evidence of a considerable risk. To that end the controller needs to prove that specific circumstances pose a concrete, considerable risk, which the controller is required to assess with special care. In order to comply with the proportionality principle, the controller, in presence of these high risk situations, is obliged to verify if possible alternative measures could be equally effective but less intrusive in relation to the aims pursued and choose such alternatives. The existence of the circumstances in question should also be reviewed on a regular basis. Based on the outcome of this review, any data processing operation that is found not to be justified any longer must be terminated or suspended*"[14].

33. The EDPS notes that the Commission evokes the considerable risk linked to firearms diversion as a justification for the processing of biometric data. Such a justification may allow for the processing of fingerprints, provided however that the Commission demonstrates concrete evidence of this risk in the relevant proposal. Similarly, the EDPS welcomes the intention that the modalities of storage of the biometric data, i.e. in the firearm, will be specified. This solution, which does not imply the creation of a central database of firearms owners' digital prints, seems legitimate and acceptable whereas storage in a central database would have required a stronger justification.

34. The EDPS still recommends a careful assessment of data protection consequences of this proposed processing. Amongst others, he insists on the necessity to identify the type of biometric data designed to identify the owner. He also recommends specifying in the proposal the security measures that should be set up to secure access to the data stored and to prevent manipulation, as well as defining the way the stored fingerprint will be changed in case of a change of owner of the firearm.

3.5. Guidance to law enforcement officers[15] and the processing of data relating to the ethnic origin of the possessor of the firearm

35. The EDPS recommends that the application and, if necessary, the update of the guidelines issued by the Council to standardise procedures concerning cross-border investigations into seized or recovered crime-related firearms[16], complies with data protection requirements for any situation where personal data processing is envisaged. In particular, he notes that the procedures presented by the Council, and the templates suggested, involve the collection of personal data relating to the

[13] Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193 adopted on 27th April 2012.
[14] See opinion 3/2012, page 13.
[15] See priority 3, task 1.
[16] See footnote 53, page 14.

possessor of the firearm and, more precisely, the collection of his or her "ethnic origin"[17] and references to his or her criminal background (which are special categories of data, as explained in section 3.2 above). Yet, there is no reference to data protection in these guidelines, although Council Framework Decision 2008/977/JHA applies.

36. In particular, due account should be taken of Article 6 of the Council Framework Decision which relates to the processing of special categories of data, which states that "*processing of personal data revealing racial or ethnic origin […] shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards*". In this regard, the EDPS recommends assessing the necessity of the processing of data relating to the ethnic origin of the possessor of the firearm to achieve the purpose pursued. He also advises that references to the rules set forth in the Council Framework Decision are inserted in those guidelines when they are updated.

3.6. Cross border cooperation to stop illegal possession and circulation of firearms

37. The EDPS notes that the plan for cross border cooperation to stop illegal possession and circulation of firearms will include coordinated collection and sharing of information on firearms crime involving police, border guards and custom authorities, both within Member States and across borders[18]. He understands that it will most probably involve the collection and sharing of personal data relating to suspects, victims and possibly brokers within cross-border national and EU level databases.

38. As a consequence, the EDPS wishes to emphasize that Council Framework Decision 2008/977/JHA will apply to these operations and specific safeguards must be developed when transfers of data to third States are foreseen. Personal data processing set up at EU level will, on the other hand, have to comply with data protection guarantees set up by Regulation (EC) No 45/2001.

39. Similarly, the Commission encourages concerted follow-up to firearms-related alerts in the Schengen Information System.

40. The EDPS welcomes the aim thus pursued by the Commission to encourage and improve the use of existing databases rather than suggest the creation of others, in line with the underlying consideration that new databases should be created only when found necessary for the purpose pursued[19].

[17] See page 13 of the Council recommendation on a standard procedure in Member States for cross-border enquiries by police authorities in investigating supply channels for seized or recovered crime-related firearms. http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2010000%202007%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F07%2Fst10%2Fst10000.en07.pdf.

[18] See priority 3, task 2.

[19] See in particular EDPS Opinion of 18 July 2013 on the proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), available in the Consultation section of EDPS website at www.edps.europa.eu

41. In this regard, he stresses that the cross-border exchange of information between official authorities within the EU should involve, as much as possible, the use of existing secured channels.

3.7. A central online repository of factual data on ballistics and weapons types

42. The EDPS notes the possibility to establish a central online repository of factual data on ballistics and weapons types to be maintained by Europol. He understands that this repository will not involve the processing of personal data, and therefore recommends that this is specified where relevant, if this is translated into concrete legislative action.

3.8. Firearms data collection plan[20]

43. The Communication notes that information on seized firearms can be logged by the police in police databases, and by customs in customs databases. Furthermore, Customs Risk Management System, the Customs Information System and the Europol Information System are not interoperable. The tasks proposed by the Commission to tackle the resulting firearms' tracing failure include the development of a firearms data collection plan and a practical solution allowing firearms experts to check against all databases of lost or stolen firearms in a single transaction.

44. Regarding the first task of developing a firearms data collection plan, the EDPS considers that this will necessarily involve the collection of personal data and therefore welcomes that his consultation is foreseen, amongst other stakeholders. This will ensure that data protection requirements, including the data minimisation principle (only data strictly necessary to the purpose pursued shall be collected) and the need to define a common and justified data retention period, are taken into account upstream and when establishing the data collection plan.

45. Regarding the second task of checking databases of lost or stolen firearms including Europol, CIS, SIS II and iARMS[21], the EDPS recognizes the legitimacy of the need to exchange information between firearms experts, whether they are police, border guards or customs agents.

46. The Commission suggests that national law enforcement applications should be updated to allow the case officer to create, update or delete records in a single transaction, which ensures that records are correct in national registers, SIS II and iArms. The EDPS understands the aim pursued which would most probably improve data accuracy, but wishes to emphasize that these developments must be made in compliance with existing rules on access to the aforementioned databases.

47. The EDPS insists on limiting access to those databases to the competent authorities and within those, to the only agents who have a "need to know". He also recommends that traceability of these designated agents' access to databases is ensured through the attribution of individual logging and passwords. In this

[20] See priority 4: Building a better intelligence picture.
[21] INTERPOL Illicit Arms Records and tracing Management System.

regard, he welcomes that Regulation (EC) No 1987/2006[22] and Council Decision 2007/533/JHA[23] already limit this access and provide for traceability. He also welcomes that access to iARMS and traceability are covered by Section 3 of Interpol's rules on the processing of data.

48. In addition, if access of new entities to the aforementioned databases were to be considered, this extension of access rights should take place under a specific legal basis, by way of an amendment of the current legal basis.

49. Finally, the EDPS recommends clarifying the modalities of the single transaction on the basis of which the creation, update and deletion of records will be made simultaneously in national registers, SIS II and iARMS.

50. According to the Communication, "any report of lost or stolen firearms should result in an alert on SIS II and iArms"[24]. In this regard, the EDPS welcomes that those two databases involve a complete traceability of the actions taken in the register by the officer, who will react to the alert or use the search tool. This will ensure that the principle of purpose limitation is respected and that strict security measures are complied with.

51. The Communication also states that "*Member States should ensure that all end-users have access to search tools currently available which enable them to make one single search to query national registers, SIS II and iARMS, with all results returned to the user's screen*"[25]. The EDPS recalls that only end-users originally authorised to access the national registers, SIS II and iArms should use these search tools and that the results returned to the user's screen shall be a 'hit' or 'no hit' reply only.

4. CONCLUSIONS

52. The EDPS welcomes that the Communication mentions that the measures planned will be implemented in full compliance with the rights to privacy and to the protection of personal data. He emphasises, however, that the processing of personal data should be reflected upon at an early stage of the legislative process and, preferably, also at the stage when the Commission adopts communications. This would help ensuring that data protection issues are identified sufficiently in advance so that, in turn, the measures to be adopted comply with data protection requirements.

53. The EDPS recommends that the data protection aspects that are relevant for the proposed measures relating to firearms are discussed during the stakeholder consultation to be carried out by the Commission. He also advises consulting the European Firearms Expert Group on data protection issues.

[22] Regulation (EC) No 1987/2006 of the European parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System.
[23] Council decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), Articles 10(b) and (f).
[24] See priority 4, task 1, page 18.
[25] See priority 4, task 1, page 18.

54. As regards future legislative proposals to be put forward by the Commission further to this Communication, the EDPS recommends that an explicit reference to the applicable EU data protection law should be inserted whenever they involve the processing of personal data. This should be done in a substantive and dedicated provision of these proposals. Pursuant to Article 28(2) of Regulation (EC) No 45/2001, the EDPS must be consulted on those proposals that involve the processing of personal data.

55. In this Opinion, the EDPS has highlighted the data protection requirements that apply to the fight against illicit firearms trafficking. He recommends that any future legislation in that area take account of data protection requirements such as necessity, proportionality, purpose limitation, data minimisation principle, special categories of data, data retention period, data subjects' rights and security of the processing. He also advises carrying out a data protection impact assessment, which will help specify the data protection safeguards to be inserted in each proposal, where necessary.

56. More specifically, the EDPS recommends that:

- any future legislative proposal concerning the establishment of an EU standard on marking should specify if any personal data will be processed, and if so, which ones and in relation to whom;

- as concerns firearms licensing the necessity of processing medical and ethnic data as well as criminal checks is assessed, and the conditions under which those special categories of data may be processed are respected, as set forth in Article 6 of the Council Framework Decision 2008/977/JHA and Article 8 of Directive No 95/46/EC. The future legislation should contain specific safeguards, such as: indicating the purpose of the processing, listing the exact types of data that can be processed, restricting access to the sensitive data only to relevant persons with a need to know and subject to professional secrecy obligations (e.g. a health professional, authorised official authorities), ensuring that the medical/ethnic/criminal grounds for refusing a license are clearly stated, and specifying the modalities for the exercise of data subjects' rights;

- the necessity and proportionality of the compulsory registration and screening of firearms brokers is sufficiently established before this measure is put in place;

- as to the possible use of biometric sensors in smart guns, evidence of the risks to security justifying the use of biometric data is provided in the relevant proposal. The proposal should indicate the types of biometric data to be processed and the security measures governing access to the data, the prevention of data manipulation and the conditions for updating the biometric data in the case of a change of owner;

- the update of the guidance to law enforcement officers should include references to the rules set forth in the Council Framework Decision 2008/977/JHA, in particular as regards the processing of special categories

of data. He also advises assessing the necessity of processing data relating to the ethnic origin of the possessor of the firearm;

- as regards cross-border cooperation, the cross-border exchange of information between official authorities in the EU should involve, as much as possible, the use of existing secure channels;

- if a central online repository of factual information on ballistics and weapons types is created, it is specified in the relevant legislation that no personal data will be processed;

- as concerns firearms data collection plan, it should be ensured that new functionalities to be introduced in national registers, SIS II and iArms are in compliance with existing rules on access to these databases. Any plan for extending the access to those databases to other entities/users should require amending the current legal base. Access to the search tool in those databases should be restricted to authorised users only and the results of these searches should be in the form of a 'hit' or 'no hit' reply.

Done in Brussels, 17 February 2014

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor