QUESTIONS ON BIOMETRIC PASSPORTS
LETTER FROM CHAIRMAN OF LIBE COMMITTEE OF 4 JULY 2007
REPLIES BY NATIONAL DATA PROTECTION AUTHORITIES[*]

Question	
1. Which authorities in your MS have or will have access to the biometric data in the passports, and for what purposes?	AUST: Apart from the passport-authorities only police, criminal judges and prosecutors have access for purposes of investigating crime. BE- Local authorities (for enrolment)and Border control (identity control) and Ministry of Foreign Affairs (identity control). CZ: Ministries of Interior and of Foreign Affairs for purpose of issuing the passports only. DE: Border police, customs authorities, passport/identity card authorities for verification purposes. After having verified the authenticity of the passport the data collected are erased immediately. MT: Passport and Civil Registration Dep (issuing authority) and police or border control for verification purposes. CY: Authorised officers of Civil Registry and Migration Dep. (issuing) and authorized members of Police[†]. GREECE: Hellenic National Passport Center (issuing authority). EESTI: Facial picture by anybody having acquired proper machine. Digital fingerprints: legally authorised authorities. SPAIN: Limited access, purpose only the management of passport control and borders. FRANCE: Under current legislation for passports, Ministry of Interior and Ministry for Foreign Affairs personnel authorised for issuing/managing the documents and authorities competent for verification and control of identity of persons (national Police, Gendarmerie, border Police and customs authorities) Under the new legislation in preparation, personnel authorised from intelligence services competent for the prevention of terrorist acts). HU: Border police/authorities. ITALY: The authorities competent for issuing passports as well as those in charge of border controls, for the purpose of "checking the passport holder's identity" in the cases provided for by law ICL: National Registry (issuer) and police or border control for identification purposes. LT: All institutions with appropriate scanning equipment will have access to the facial picture. Fingerprints a limited number of authorities. Current legal acts do not foresee what authorities may have such access. Currently competent institutions are discussing what institutions will be able to access the biometric data in passports. LATVIA: All authorities, based on a legal obligation to carry identification.

[*] This table summarises the contributions provided to the Secretariat of the Article 29 Working Party by 6 December 2007. UK are Ireland are not bound by Regulation 2252/2004/
[†] CY: Recent press releases inform that competent authority would be the Ministry of Justice and Interior and the Police would be the issuing authority.

	LUX: Currently only the Ministries for Foreign Affairs and Interior (Visas, Passports and Legalisations Offices) have access to biometric data of LUX citizens. The facial photo and signature are electronically enrolled and they are deleted from the system after one month. The same procedure could be applied to digital fingerprints as from 2009. SL.: Authorized border authorities. SK: Legislation in preparation, but at this stage only the Policy for the performance of its tasks. NL: All authorities that, based on a legal obligation to carry identification, are authorised to ask for ID. ROM: Passport Issuing authority and Public services for issuing and managing data bases for simple passports and Border Police (verification). SWEDEN: Police and other authorities responsible for border controls. FINLAND: border guard, police and ministry of foreign affairs for verification of the document and identity of the holder. IRL: The biometric template generated from the full frontal image is stored in the passport database and no other authority in Ireland will have access to it. **EEA Countries** ICL: National Registry (issuer and police or border control for identification purposes. NORWAY: Legislation in preparation, too early to reply.

2. Where are biometric data stored in addition to the passport/travel document? (in a decentralised way or in a central data base)?	**Decentralised (Chip support)** NL. DE: Fingerprints only chip support (DE as of 2009)) SWE- The digital photo is stored in chip in the passport. A copy of the digital picture is also stored in the National Police Board's passport data based called "Passregister". IT: Biometric data will only be stored in the chip located in the passport cover; no storage in a centralised database is envisaged. LT (as of 2008) and seem to be decentralised FR (current electronic passport only a picture and no fingerprints. Not stored n a central system) .	**Centralised** BE: Ministry of Foreign Affairs CY: They will be stored in a central data bases. CZ (but does not serve to identify persons). SK: Ministry of Interior, with decentralize data bases for operational purposes with the police, ministry of Foreign affairs. SL, SPAIN, FRANCE The present central data base does not include any picture up to now; under the legislation in preparation, it would include both the digital picture and fingerprints EE: Citizen and Migration Board**;** Passport Department: ROM, Greece, FIN (picture and signature in the passport information system) LATVIA: central data base **Picture only** DE: picture stored in passport authority LUX: Biometric data are stored in a central data base at the Passports Bureau. No decision taken yet with regard to fingerprints. However it has not yet been decided whether passport applications will be made to municipal authorities or to some regional offices set up for this. HU passport data base does not have a specific sub-database for biometric data. But all passports are centralized. AUST: The digital photos, which are so far the only biometric data contained in Austrian passports, are stored in the Central ID-Register. Whether this will be true also for fingerprints after their introduction into passports is a highly sensitive question which has not at all been decided yet. IRL: The biometric template and the full frontal image are stored in a central database (Not bound by Regulation 2252/2004**).**

3. Whether the MS have the intention to go further and require other biometric data	**Only those biometric data required by Regulation 2252/2004 (e.g. picture and fingerprints)**: AUST, BE, LUX, NL, SL, GR, SK, DE, LT, ROM, MT, EE, FIN, CZ, CY, HU, LUX; SWE, IT (at this stage only the picture is required and stored in the chip) **EEA Countries:** ICL FR: under a new legislation in preparation, it is planned to have both the digital picture and fingerprints integrated in the electronic component. The central data base would include both the digital picture and fingerprints. IRL: Ireland is not part of the Schengen Acquis and is not obliged by the EU directive to include a second biometric. At present the Irish Government has no plans to add a second biometric but will monitor closely the developments in this regard. *(See below question 9 on the timetable for the introduction of biometric requirements in EU passports)*

4.- Provisions taken by MS in case of problems of enrolment (eg. lack of fingerprints or false rejections	**Technical specifications not yet adopted :** ROM FR will adopt measures when fingerprints will be included in passports LUX: Measures for specific cases (eg.: lack f fingerprints, children or old persons) not yet defined SL adopted when fingerprints will be in passports (2009) FIN when fingerprints taken procedures to be developed in case they are not available No practical problems yet as no fingerprints taken (MT, LT, EE, FIN and ICL) **No information available yet:** SWE, LTV, AUST GR: under analysis. **Specific measures:** BE: In conformity with ICAO rules, a non-working ePassport remains a valid travel document. In case of non-functioning of the biometrics, the control has to be done in a classical way. CZ: In case of problems with enrolment of fingerprints (based on anatomical or physiological changes or due to health handicap) the travel document without fingerprints data will be issued. (Compliance with ICAO 9303). The data medium will include biometric facial image only together with information on impossibility to enrol the fingerprints. CY: Compliance with the appropriate EU Regulation and ICAO document 9303. HU: If mistakes found in passport a new passport to be issued. IT: If no fingerprints are available because of mutilation and/or the fingerprints are illegible because of skin problems, no fingerprints shall be collected DE: Training of officials for enrolment and verification. If failure border control takes place as usual. NL: If not possible to enrol fingerprints they will not be enrolled. SK: If problem to enrol, passport issued without biometrics and a comment inserted in the passport. IRL: Where citizens, through any sort of injury or disability cannot conform to the photographic requirements, the passport Office will deal privately and sensitively with the individual. A full frontal image may not be possible but a best attempt will be made. This will be apparent to an immigration officer on presentation of the passport. A lack of fingerprints is not an issue. LV: If fingerprint cannot be taken then passport will be issued without digital pictures of fingerprints according to regulatory enactments SPAIN (no reply)

5. Experience of MS with encryption rules for the data on the storage medium and access control and extended access control for fingerprints. Can these rules ensure security against skimming and eavesdropping? (In Belgium it seems that passports were not encrypted)	AUST: No information available yet. BE: Since technical specifications of the Commission were not available at the time, Belgian ePassports of the first series (issued from November 2004) were only protected with the (not compulsory) Active Authentication. When the technical specifications became available, Belgium added the Basic Access Control. CZ- no fingerprints taken yet. Measures in preparation although DPA not involved. No serious problems I current practice so far. **CY: Encryption will be used.** EE, LATV: rules encryption to be implemented DE: Basic and extended access control implemented. For fingerprints Extended access control and only authorized official institutions able to read them. Strongly encrypted channel between chip and machine to avoid eavesdropping. SPAIN: High security measures FR: raises some questions as the RFID chip used is not completely safe (no internal clock, week encryption power) and unlawful access could be possible. No real experience yet, limited to travel documents. The session number of the reading operation is "random" to prevent tracking of personal data. FR plans to include protection measures against skimming and sniffing attacks in future implementations of the passport HU: encryption. If attempt to alter data made, data will be destroyed and no use of the medium possible. IT. No available information. Data are encrypted but EAC not implemented as fingerprints are not yet taken. LUX: Currently biometric passports are encrypted (Basic Access Control) following Commission and Article 6 Committee Decision. Measures for setting up Extended Access Control have been started to be developed. LT: when fingerprints implemented there will be extended access control and only certified equipment strictly controlled will be able to read it. Only authorised authorities will have required coded for scanning. MT- Data in the document shall be encrypted. NL: active authentication and basic access control used. No problems so far. When fingerprints implemented extended access control adopted SK : encryption ROM- No experience SL: ICAO recommendations (digital signature of data stored in chip issued by the SL certification authority. SWE- passive authentication used today and basic access control for the picture. For fingerprints probably active authentication and extended access control.

	FIN: unauthorised access prevented by adequate technical rules; methods used are the most efficient security when possible. **IRL: Not applicable** **EEA Countries: ISL**: Extended access control not implemented as fingerprints are not taken. Of Course, when fingerprints will be added (June 2009 at the latest), Extended Access Control will be implemented too

6. Do Member States consider giving access of fingerprints to third countries by the extended access control?	NO BE- Only to EU Member States CY Not at present GR, LT. NL, ISL no decision taken yet FIN- no discussions yet at national level. SWE, MT: No information available SK-No access granted to third countries IT: No available information yet. At all events, any co-operation mechanisms within and outside Europe as regards law enforcement authorities have to be discussed and approved beforehand at national and/or supranational level by the competent bodies LUX. Not decided yet, but probably No. LATVIA: Not at present. All access will be granted regarding EU legislation only. SL, CZ: does not seem to be the case. AUST- No information available yet. IRL: Not applicable.	YES DE: In principle yes, although no EU or bilateral regulations exist yet. EE- considering it; but not decision taken yet. SPAIN: according to international treaties or conventions FR: the risk exists that third country authorities process such data by means of devices interoperable. HU: within existing agreements on international assistance ROM: considering it by the extended access control

7. In the absence of a central European matching system will each MS set up its own matching system? How efficient will these systems be, in particular which false rejections will be defined?	**YES** **Not decided yet**: BE, MT, EE, GR, FIN, NW, NL **No information from Ministry of Interior:** LT No information available: SWE IT: No available information. Account should be taken, at all events, of the existence of a widely tested matching mechanism within the framework of the SIS/SIS II as for stolen passports; co-operation mechanisms are also in place as regards Interpol. CZ: There are legal provisions enabling creation of a national matching system, but not yet applied. LAT: to be decided on implementing rules. SL: to be established soon. SL: no clear question, but does not seem necessary to have a central matching system To assess in operational tests: It is expected that compliance of fingerprint images and fingerprint acquisition/matching equipment with the standards foreseen by the technical amendments of Directive (EC) 2252/2004 should guarantee a sufficiently efficient fingerprint matching. (DE) To be established soon: SL HU: employ AFIS system on crime and immigration control areas. LUX-Early to reply. This matter needs to be discussed yet.	**NO** CY: there will be one-to-one matching FR the present central data base does not include any biometric data; but under the legislation in preparation, a central database would be implemented providing for a possible 1-1 authentication but no identification query by biometric data could be performed (i.e. It would not be possible to identify a user by submitting his fingerprints to the system). IRL: If this is a central fingerprint database it does not apply to IRL. SK LUX: Difficult to reply at this stage. AUST: No information available yet.

8. Do MS envisage to adapt these rates according to the circumstances, for example in case of higher security risks?	YES FR: No available at present. HU: If there is legal authorisation HU: possibility of increasing the efficiency must be examined DE: testing on going to assess and fix a value of False Acceptance Rate.	No decided yet: GRE, FIN, EE, NL, MT, ISL, RO; SL. SK: Not now since absence of electronic matching system. No available information: IT, CZ, SWE, AUST. No reply: CY, NW, SPAIN SL, LIT. IRL, LUX: see reply to Question 7.

9.- Each MS must give an overview of their timetable for the introduction of biometric passports.	BE: face already in force since 11/2004	Fingerprints by June 2009
	CZ- Picture: September 2006	Fingerprints February 2008‡
	CY: 12 months	
	DE: Photograph 1.11.2005.	Fingerprints: 1.11.2007
	EE: picture: 22.5.2007	Fingerprints 2009
	GRECE: 2006 picture	Fingerprints in 2009
	SPAIN: picture 2006.	Fingerprints??? (no information provided)
	FR: picture already in place and the deployment for other biometric elements should begin in October 2008 to ensure generalization possibly by June 28, 2009.	
	HU: Picture form 1.9.2006.	Fingerprints 1.8.2009
	IT: Picture already in place	Fingerprints: Not decided yet, but within the deadline required by Regulation.
	Latvia: Photograph: November 20th, 2007	Fingerprints: July 1st, 2008.
	LT: passports with picture: 28.8.2006.	Fingerprints 28.6.2009
	LUX:	Fingerprints 28.6.2009
	NL: Picture 26.8.2006	Fingerprints 28.6.2009
	ROM: entry into force 1.1.2008	
	SL: picture: June 2006	Fingerprints June 2009
	SK: picture: 1.1.2008	Fingerprints : June 2009
	SWE: passport with digital facial photo stored in a chip since October 2005	
	FIN picture, already in a chip.	Fingerprints 2008
	MT: Not yet decided	
	IT: no information available with regard to the inclusion of fingerprints. Although IT intends to comply with Regulation 225/2/2044.	
	AUST: Picture: already in place	Fingerprint: deadlines will be met.

‡ CZ (according to recent press information the date will be delayed until 1.4.2009;

	EEA Countries: ISL: Passport with fingerprints to be issued. No date yet fixed NW: No information available.

10.- Any other issues you consider important	IT: It would be appropriate to seek Europe-wide co-ordination as for clearly setting out mechanisms and procedures to introduce and manage biometric passports, taking account of the need to prevent the establishment of centralised databases (see WP29's opinions on the use of biometrics, in particular in passports). HU: Some of the questions refer to the interoperability of administrative and criminal data. As these fields have different purposes, their interoperability may not be automatic from a data protection aspect. In case it is provided for by an act, the possibilities and conditions of the feasibility should be examined. SW: The questions raised are focused on the practical introduction of e-passports and technical standards for security and access control. The Federal Office for Information security (BSI) has published the Extended Access Control (EAC) in a technical guideline. FR: CNIL draws the attention on the fact that the option can be made in favour of storing fingerprints instead that "minutiae" These options could be examined in view of technical solutions existing and against possible advantages or risks they may present.

NW- on going legislation not able to reply. DK: No information available to the DPA.