EUROPEAN
COMMISSION

Brussels, 6.4.2016
SWD(2016) 115 final

PART 3/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Annexes to the Impact Assessment report on the introduction of an 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)

{COM(2016) 194 final}
{COM(2016) 196 final}
{SWD(2016) 116 final}

Table of Contents

10. ANNEX 10: IMPLEMENTATION COSTS AT NATIONAL LEVEL

For the implementation of Smart Borders in the 30 Member States, the structure used is the so-called "MS Toolbox" developed during the Technical Study in 2014. The cost computation is done independently of the funding, as it might very well be that some of the Member States considered would not be eligible for EU funding programmes. However the incurred cost would remain.

Given the scope of the proposed Smart Borders system there are only costs at the border and none at the consulates.

The technical integration of NUI (National Uniform Interface) with national systems is already included in the estimate of the Smart Borders system, which explains why these costs are computed here.

The national investments are computed as marginal costs on top of the existing personnel and infrastructure.

10.1. Set-up costs at Member State level

The following cost items are considered:

Nbr	Work/Description	Quantity	Unit Price (in k€)	Total (in k€)	One-off or recurrent
1	Project Management of transformation of each border type: processes, people and technology	46	462	21.252	One-off
2	Procurement of new border equipment installations	30	88	2.640	One-off
3	Training of 1st line border guards	20.000	0.2	4.000	One-off
4	Changes to national border control application	30	220	6.600	One-off
5	Enhancement of national IT infrastructures	30	750	22.500	One-off
	Total			**56.992**	

Assumptions:

Item 1: use of two internal (€350/day) and two external staff (€700/day) during one year (220 days) (so 2 x (350 + 700)*220=462 k€). This number is multiplied by 46 which represents the number of Member States multiplied by the number of different types of border per country. When a county has multiple types of border, 50% and 25% of the cost is counted for second and subsequent border type.

Item 2: Use of two internal resources (€200/day) during one year (220 days) (in total 88k€) and multiplied by the 30 (one per Member State).

Item 3: Training of border guards in first line: two days at daily cost of €100/day (in total 0.2k€) applied to 20.000 persons.

Item 4: Changes to end-user systems to include Smart Border processes. Estimate of two persons (value €500/day each) during one year (220 days), for a total of 220k€ development cost per Member State.

Item 5: Enhancement of national network and infrastructure. Estimate of 750k€ to cope with increased network traffic per Member State.

10.2. Costs for Border Equipment

There are about 1.800 border crossing points for the 30 Member States considered. However many of them are of small and even very small size like airfields and harbours for leisure boats. The estimate is that there only 127 large border crossings (7% of the total): 40 sea border crossings, 27 airports, 40 land borders and 20 railway connections linking Schengen countries (including countries that do not yet completely implement the Schengen acquis) and third countries.

Equipment cost for small border crossings

For a small border crossing the assumption is made that there are only two desks (either entry/exit or EU/non-EU).

The equipment necessary for a small border crossing is:

Equipment	**Quantity**	**Price (in €)**	**Total (in €)**
Passport reader –fixed (including authentication)	2	1.500	3.000
Equipment for taking facial image	2	500	1.000
4 FP reader[1]	2	4.000	8.000
Total			12.000
Yearly maintenance of 10%			1.200

The **total cost for equipment of the small border crossing points** would amount to **€20,16 million** (1680 border crossing points @ 12.000€/case). This investment would induce an **annual maintenance cost of around €2 million**.

Equipment cost for large border crossings

For the large border crossing points the assumption differs according to the type of border crossing.

Equipment	**Quantity**	**Price (in €)**	**Total (in €)**
Air border entry			
Equipment for the manual lanes			
Passport reader –fixed (including authentication) -	0	Assumed to be already available	0
Equipment for taking facial image	6	500	3.000

[1] The unit price is a generous one as the information on average prices done as part of the Smart Borders pilot indicate ranges of average prices between €1.000 and €16.643. Differences relate to whether the device can be used standalone or integrated, and whether it is a contact device or a contactless one. In this cost computation the fingerprint reader is assumed to be a contact device.

4 FP reader	6	4.000	24.000
Sub-Total			***27.000***
Yearly maintenance of 10%			***2.700***
Equipment for automated lanes			
3 kiosks for each of 6 entry lanes for non-EU citizens	18	25.000	***450.000***
Yearly maintenance of 10%			***45.000***
Air border exit			
Additional e-gates for non-EU citizens.	6	75.000	***450.000***
Yearly maintenance			***45.000***
Total per Air border			**927.000**
Yearly maintenance			92.700

Equipment	**Quantity**	**Price (in €)**	**Total (in €)**
Sea border entry –fixed equipment			
Passport reader –fixed (including authentication)	0	Assumed to be available	0
Equipment for taking facial image	6	500	3.000
4 FP reader	6	4.000	24.000
Sub-Total			***27.000***
Yearly maintenance of 10%			2.700
Sea border entry mobile equipment			
Mobile stations	6	15.000	***90.000***
Yearly maintenance of 10%			9.000
Sea border exit			
Additional e-gates	6	75.000	***450.000***
Yearly maintenance			45.000
Total per Sea border entry Assume 50% fixed and 50% mobile			**58.500**
Yearly maintenance			5.850
Total per Sea border exit			**450.000**
Yearly maintenance			45.000

Equipment	**Quantity**	**Price (in €)**	**Total (in €)**
Land border entry –fixed equipment			
Passport reader –fixed (including authentication)	6	Assumed to be available	0
Equipment for taking facial image	6	500	3.000
4 FP reader	6	4.000	24.000
Sub-Total			***27.000***
Yearly maintenance of 10%			2.700
Land border entry mobile equipment			
Mobile stations	6	15.000	***90.000***

Yearly maintenance of 10%			9.000
Total per Land border entry Assume 50% fixed and 50% mobile			**58.500**
Yearly maintenance			5.850
Total per Land border exit			**58.500**
Yearly maintenance			5.850

Equipment	**Quantity**	**Price (in €)**	**Total (in €)**
Railway border mobile equipment			
Mobile stations	4	15.000	***60.000***
Yearly maintenance of 10%			6.000
Total per Railway border			**60.000**
Yearly maintenance			6.000

	Number of border crossings	**Average investment cost (in k€)**	**Investment (in k€)**	**Yearly maintenance in k€**
Air borders	27	927,0	25.029	2.502,9
Sea borders (entry and exit)	40	508,5	20.340	2.034,0
Land borders	40	117,0	4.680	468,0
Railway connections	20	60,0	1.200	120,0
Sub-Total	***127***	***403,5***	***51.249***	***5.124,9***
Integration cost (IT investment and infrastructure changes) at the level of the border post	127	300,0	38.100	0
Total	**127**	**703,5**	**89.349**	**8.934,9**

The **total cost for equipment of the large border crossing p**oints would amount to €**89,35 million**. This investment would induce an **annual maintenance cost of almost €9 million**.

10.3. Summary and timing of Implementation costs

The implementation cost on Member States side would consist of:

– €57,0 million set-up costs over the 3-year development period. This will be split as €10 mio the first year, €20 mio the second year and €27 mio the third year as the lead time for procurement under new contracts will make that the amounts of investment will mainly take place from the second year.

– €109,5 million (20,16 + 89,35) equipment cost for small and large borders to be done over the 3-year development period. This is a simplification these investments could also be done beyond the development period as the most expensive equipment are

process accelerators and could also be implemented only when the number of border crossings increases, meaning years 4 and 5. The investments would be split as €20 mio the first year, €40 mio the second year and €49,5 mio the third year. This investment would induce an annual maintenance cost of 10% on the accumulated investment and would reach €11 million (2+9) once completely accomplished.

In mio €	1st year	2nd year	3rd year	4th year	5th year	6th year	7th year
	Development period			Operations period			
Investment	10	20	27	0	0	0	0
Equipment	20	40	49,5	0	0	0	0
maintenance		2	6	11	11	11	11
Total	**30**	**62**	**82,5**	**11**	**11**	**11**	**11**

11. ANNEX 11: BENEFITS OF SMART BORDER PREFERRED SOLUTION

This annex details the origin of the benefits of the preferred solution, an assessment of their magnitude and the assumption for "monetizing" (meaning computing a monetary value to it) them when possible.

The approach starts from the list of impacts in chapter 6 of the Impact Assessment, uses the assessment made in the comparison of options in chapter 7 and details the assumptions for estimating the magnitude of the benefit.

The computation of benefits is explained first and the benefits computed in a sheet.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
1	**Social Impact impact on third country nationals (see 6.1)**	**Border crossing time at entry:** • No impact for visa-required travellers not using facilitation. • *Negative impact for visa-exempt travellers at first enrolment.* • No impact for enrolled visa-exempt travellers. • *Positive impact for travellers using the "Fastlane for All"* **Border crossing time at exit** • No impact on exit time for all travellers	*Negative impact for visa-exempt travellers at first enrolment* When a 5-year data retention period is assumed, all visa-exempt travellers will need to be enrolled the first year. The next years this number decreases quickly as data is retained for 5 years and only not yet registered travellers need to be enrolled. The Smart Borders pilot showed that enrolment using the preferred solution would add 30 seconds + system response of 10 seconds to the existing border crossing time. The enrolment process adds therefore about 40 seconds (0,7 minutes) to the border crossing time but about 10 minutes to the dwelling time in the busy border posts (which is a reasonable value). An estimated 70% of travellers use the busy border crossing points. The opportunity cost for the additional time spent for crossing the border is valued at a standard cost of €31[2] per hour. Value = proportion to be enrolled (from 1 to 0,20) x 0,70 x number of TCN-VE x 10 min x 31 €/60min *Positive impact for travellers using the "Fastlane for All*" An estimated 70% of travellers use the busy border crossing points. The percentage of travellers using the "Fastlane for All" would start from 30% in 2020 and reach 70% in 2025, which has been demonstrated to be realistic

[2] Value taken from "Standard Inputs for Eurocontrol Cost Benefit Analysis" version 6.0 of September 2013, page 31 where the passenger value of time is rated at 31€/hour by General Aviation. This is below the recommended value of €47 to €60 per hours per passenger recommended by Eurocontrol.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
			based on implementations in Canada and USA. The benefit per traveller is estimated as 5 minutes less dwelling time (which is a cautious estimate and inferior to the added duration of enrolment), valued at the same rate as above. Value = (0,30 to 0,50) x 0,70 x number of TCN border crossings/year x 5 min x 0,50 €/min
2	**Economic impacts impact on transit hubs (see §.2).**	Fastlane for all reduces the cost of delay for lost connections.	There is no estimate for this benefit.
3	**Impact for Border Control Services**	**Workload for border guards:** • Additional workload for enrolling visa-exempt third-country nationals in congested border crossing points. • Reduced workload for controlling third country nationals using "Fastlane for All".	*Additional workload for enrolling visa-exempt traveller.* Only in congested border crossing points will an increased workload lead to a need for more staff. In a non-congested border crossing point will an increase in workload reduce the idle time. When a 5-year data retention period is assumed, all visa-exempt travellers will need to be enrolled the first year. The next years this number decreases quickly as data are retained for 5 years and only not yet known travellers need to be enrolled. The enrolment process adds 40 seconds (0,7 minutes) to the border crossing workload. Maximum 70% of travellers will use the congested border crossing point. The cost for the additional time spent for crossing the border is valued at a standard cost of €40 per hour. Value = proportion to be enrolled (from 1 to 0,20) x 70% x number of TCN-VE x 0,7 min x 40 €/60min =.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
			Reduced workload for controlling third country nationals using "Fastlane for All" About a third of the border crossing workload is shifted to the travellers. In busy/congested border crossing points a decreased workload per traveller will lead to the possibility to control more travellers per border guard. The percentage of travellers using the "Fastlane for All" would start from 30% in 2020 and reach 70% in 2026. This is a slow pattern of uptake. From the Smart Borders Pilot the benefit per controlled traveller is estimated between 0,60 minutes (36 seconds) and 1 minute per traveller[3] at entry and 36 seconds (0,6 minutes) at exit, valued at the average rate of 40€/hour. To remain cautious the lower value of 0,60 minutes is kept at entry. Value in time = (0,30 to 0,70) x number of TCN border crossings/year et entry x 0,60 min x 40 €/60 min + (0,30 to 0,70) x number of TCN border crossings/year et exit x 0.6 min x 40 €/60 min
4.	**Impact for Immigration Enforcement**	**Identifying overstayers:** • Additional income from fines on identified overstayers **More efficient and effective and identification of irregular migrants:**	*Additional income from fines on identified overstayers* As overstayers will be systematically identified at the border, the revenue of fines imposed by MS will increase. The assumption is made that 1 person out of 1.000 overstays more than 7 days and that the average fee amounts to €10 per day.

[3] One minute is the estimated upper limit of benefits according to the Smart Borders pilot result. This value corresponds to the benefit of 1 minute per border guard and per controlled traveller computed from the figures cited in a presentation by the US Customs and Border Protection in 2014, citing "Global Entry members have used the kiosks over 13 million times, saving 208.000 officer hours", which makes that 208.000 hours x 60 min/hour/13 million = 0,96 min/entry, rounded to 1 minute.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
		• The saved cost of not having to increase the Immigration enforcement services staff to identify more irregular migrants. **More efficient and effective implementation of return decisions:** • Saved cost of executing a higher proportion of return decisions.	Additional revenue = (number of travellers per year) x 7 days x 10 /1000 = a figure comprised between €3 and 5 million for current Schengen countries. *Saved cost of not having to increase the Immigration enforcement services staff to identify more irregular migrants*. The number of regular migrants becoming irregular migrants by overstaying is estimated at 250.000 persons. The Smart Borders system would provide a reliable tool for identifying more overstayers without increasing the staff number. The assumption is made that after one year, 5%, than increasing from 10% till 16% more migrants in irregular situation will be identified per year and that currently 8 migrants are identified per immigration control staff and per year. The saved cost= (5% till 16%) x (250.000 per year) x Yearly cost of law enforcement officers /8. The yearly cost of law enforcement officers is estimated at €45.000/year[4]. This cost is consistent with the hourly cost used for calculating the cost of the additional work for border guards. *Saved cost of executing a higher proportion of return decisions*. Only 50% out of 250.000 return decisions are implemented. This number of return decisions is kept constant over time which is a cautious estimate. This means that the staff cost incurred for preparing and executing the return

[4] This figure is consistent with the value given in a presentation called "Risk Analysis and Electronic Lodgement to Improve Border Management where the identification of one overstayer was estimated to cost 60.000 AUD (Australian dollars), which equates €45.000. The figure was obtained by dividing the budget line for these activities by the number of people this activity applied to.

	Category of impacts (from chapter 6 of the Impact Assessment)	Impact on	Estimation + Value and timing
			decision is lost in one case out of two. The assumption is made that the execution of a return decision requires 20 hours of work valued at €30 per hour. Assume the proportion of effectively executed return decisions increases from 4% to reach 33%, than the benefit is. Value= (4% to 33%) x 250.000 x 20 hours x €30/hour= €6 to 49,5 million according to the year.
5	**Impact for Law Enforcement**	Use as criminal identification tool. Use as criminal intelligence tool	The benefits of being able to use the system as a criminal intelligence tool and criminal identification tool are not expressed in a financial value. The benefits are • As a criminal identification tool: reduce the cost of more resource-intensive means to identify persons. • As a criminal intelligence tool: contribute to faster crime resolution or avoidance of criminal acts. There is no estimate for this benefit
6	**Air and sea carriers**	Reduction of the risk of incurring a fine and a penalty for having transported travellers to the Schengen border who are refused entry	The system will also include a web-site for carriers that will allow them to check whether the traveller meets the entry conditions for the Schengen area. However, the traveller can still be refused entry on the basis of other ground and the traveller is then case still liable for bringing the traveller back to the place of departure. There is no estimate for this benefit.

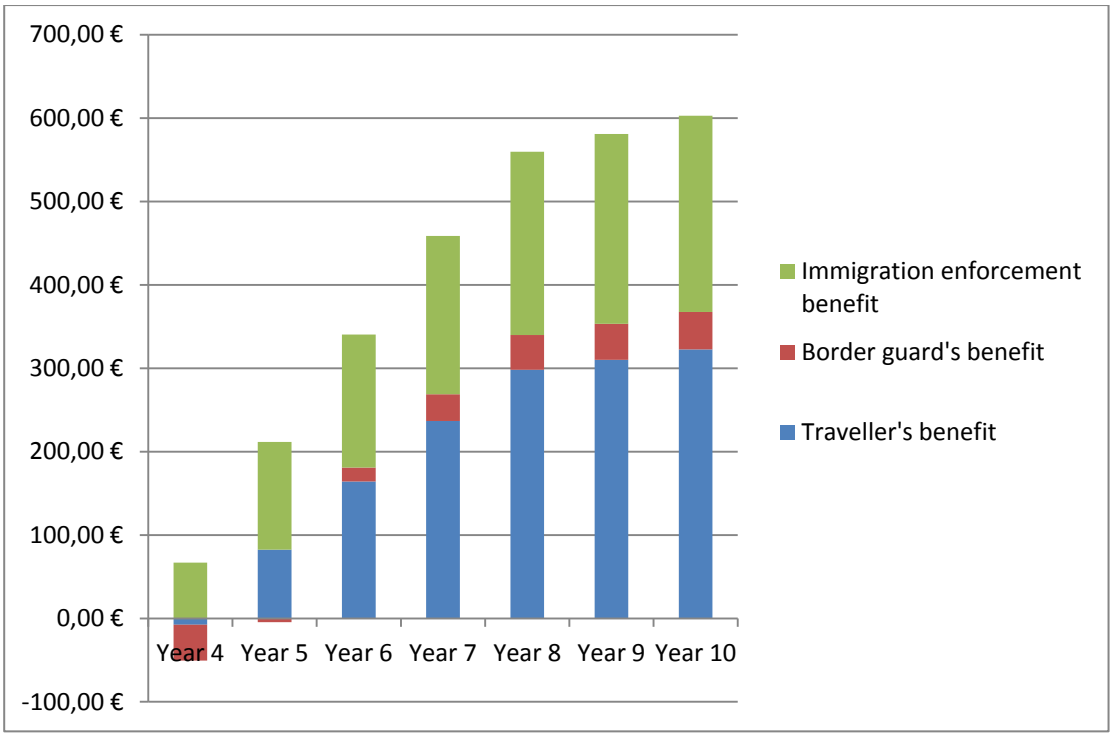
Graphical representation

The following graphs represent the distribution of benefits over time and split over the three main areas:

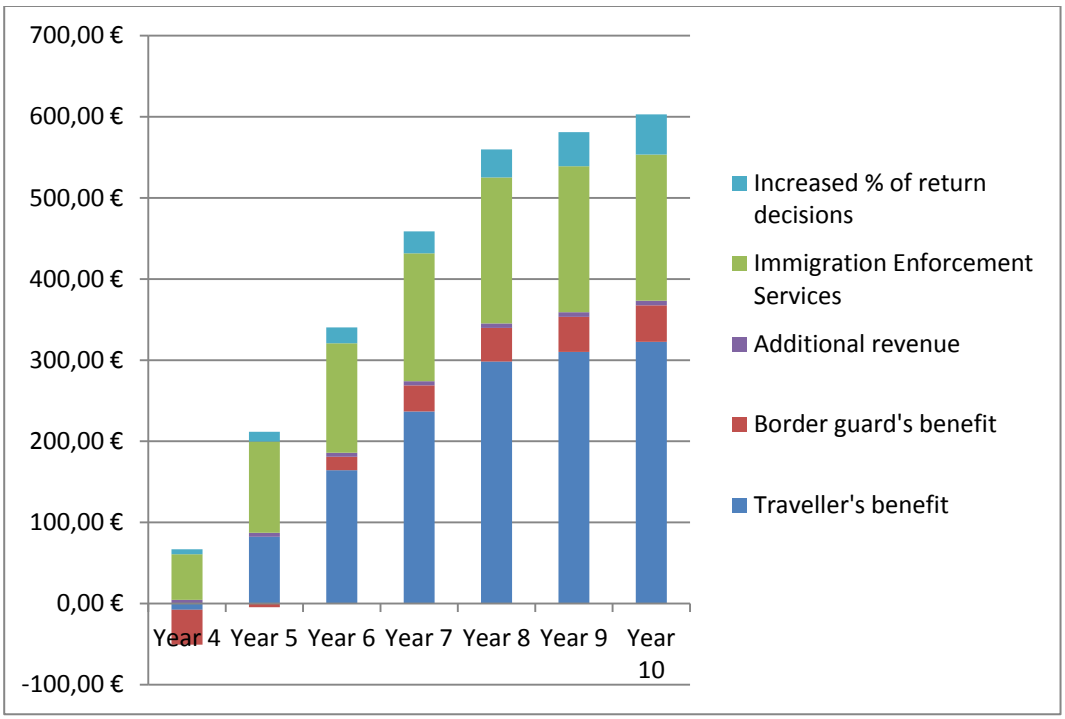
– Benefits for the traveller obtained as a reduction of the dwelling time despite an increase of border crossing time for the visa-exempt travellers who need to be enrolled again. The benefits stem from the use of self-service kiosks for an increasing proportion of travellers.

– Benefits for border guards in terms of saved workload. The first year this benefit is negative as a vast majority of visa-exempt travellers need to be enrolled. The second year this benefit is close to zero and becomes positive in the next years. This benefit pattern is the consequence of having to enrol a lower proportion of travellers.

– Benefits for immigration enforcement which has different components: additional income from fines on identified overstayers (additional revenue), the increased effectiveness of immigration enforcement services (Immigration Enforcement Services), the saved cost of better execution of return decisions. This detail is provided on the second chart.



X-axis: year after project start. First three years are for development and no benefits are generated over that time
Y-axis: benefits in million € per year.



X-axis: year after project start. First three years are for development and no benefits are generated over that time.
Y-axis: benefits in million € per year.

Cost-Benefit Estimation	Development year 1 2017	Development year 2 2018	Development year 3 2019	Operations Year 1 2020	Operations Year 2 2021	Operations Year 3 2022	Operations Year 4 2023	Operations Year 5 2024	Operations Year 6 2025	Operations Year 7 2026
	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Costs										
Development and Operations of Smart Borders		Part highlighted represents the €480,2 million of financial annex								
Central System					26,32	27,07	27,43	27,43	27,43	27,43
National systems					19,71	19,71	19,71	19,71	19,71	19,71
Total	112,65	115,60	206,52	45,47	46,03	46,78	47,14	47,14	47,14	47,14
Changes SIS II and VIS	0			0	0	0	0	0	0	0
Total Development and Operations of Smart Borders	**112,65**	**115,60**	**206,52**	**45,47**	**46,03**	**46,78**	**47,14**	**47,14**	**47,14**	**47,14**
Compliance costs MS (see Annex 10)	30	62	82,5	11	11	11	11	11	11	11
Total Costs	**142,65 €**	**177,60 €**	**289,02 €**	**56,47 €**	**57,03 €**	**57,78 €**	**58,14 €**	**58,14 €**	**58,14 €**	**58,14 €**
Cumulated Costs	**142,65 €**	**320,25 €**	**609,27 €**	**665,74 €**	**722,77 €**	**780,55 €**	**838,69 €**	**896,83 €**	**954,97 €**	**1.013,11 €**
Benefits										
Parameters										
TCN-VE border crossings per year (in million)	92	96	100	104	108	112	117	122	127	132
TCN-VH border crossings per year	126	131	137	142	148	154	160	166	173	180
TCN border crossings per year (in millions)	219	227	237	246	256	266	277	288	299	311
TCNE-VE (in million)	34,7	36,1	37,5	39,0	40,6	42,2	43,9	45,6	47,4	49,3
TCN-VH (in million)	24,0	25,0	26,0	27,0	28,1	29,2	30,4	31,6	32,8	34,2
TCN (in millions)	58,7	61,0	63,5	66,0	68,6	71,4	74,2	77,2	80,3	83,5
Border crossing time at entry										
Proportion of VE travellers to be enrolled	0	0	0	1,00	0,70	0,50	0,40	0,40	0,40	0,40
Proportion of travellers passing via busy BCP's	0	0	0	0,70	0,70	0,70	0,70	0,70	0,70	0,70
Increased dwelling time (min)	0	0	0	10	10	10	10	10	10	10
Average opportunity cost (per hour)	0	0	0	31 €	31 €	31 €	31 €	31 €	31 €	31 €
- impact for VE travellers at first enrolment	*0*	*0*	*0*	*141,05 €*	*102,68 €*	*76,28 €*	*63,46 €*	*66,00 €*	*68,64 €*	*71,39 €*
Proportion of border crossings using kiosks	0	0	0	0,30	0,40	0,50	0,60	0,70	0,70	0,70
Reduction in dwelling time (min)	0	0	0	5	5	5	5	5	5	5
+impact for travellers using fastlane		*0*	*0*	*133,46 €*	*185,06 €*	*240,57 €*	*300,24 €*	*364,29 €*	*378,86 €*	*394,01 €*
Border crossing time benefit in million € - Traveller's benefit	**0**	**0**	**0**	**-7,60 €**	**82,37 €**	**164,30 €**	**236,77 €**	**298,28 €**	**310,22 €**	**322,62 €**

Impact for Border Control Services										
Proportion of VE travellers to be enrolled	0	0	0	1,00	0,50	0,30	0,20	0,20	0,20	0,20
Proportion of VE travellers enrolled at busy BCP's	0	0	0	0,70	0,70	0,70	0,70	0,70	0,70	0,70
Increased workload for border guards (min)	0	0	0	0,7	0,7	0,7	0,7	0,7	0,7	0,7
Average cost (per hour)	0	0	0	40 €	40 €	40 €	40 €	40 €	40 €	40 €
Cost of Additional workload for enrolling VE travellers (in millions)	*0*	*0*	*0*	*63,70 €*	*33,12 €*	*20,67 €*	*14,33 €*	*14,90 €*	*15,50 €*	*16,12 €*
Proportion of travellers using kiosks	0	0	0	0,30	0,40	0,50	0,60	0,70	0,70	0,70
Reduction in workload for BG's per border crossing at entry (min)	0	0	0	0,6	0,6	0,6	0,6	0,6	0,6	0,6
Reduction in workload for BG's per border crossing at exit (min)	0	0	0	0,6	0,6	0,6	0,6	0,6	0,6	0,6
Benefit of Reduced workload when TCN's using fast lane for all	*0*	*0*	*0*	*20,66 €*	*28,65 €*	*37,25 €*	*46,49 €*	*56,41 €*	*58,66 €*	*61,01 €*
Benefit on Border Control Services (in million €) **- Border guard's benefit**	**0**	**0**	**0**	**-43,04 €**	**-4,47 €**	**16,58 €**	**32,16 €**	**41,50 €**	**43,16 €**	**44,89 €**
Impact for Immigration Enforcement										
Number of travellers per year	0	0	0	66,0	68,6	71,4	74,2	77,2	80,3	83,5
Proportion of overstayers	0	0	0	0,001	0,001	0,001	0,001	0,001	0,001	0,001
Average duration of overstay (in days)	0	0	0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
Average fine per day	0	0	0	10,00 €	10,00 €	10,00 €	10,00 €	10,00 €	10,00 €	10,00 €
Additional revenue (in million €)	***0***	***0***	***0***	***4,62 €***	***4,80 €***	***5,00 €***	***5,20 €***	***5,40 €***	***5,62 €***	***5,85 €***
Number of overstayers (persons) - medium value	0	0	0	250.000	250.000	250.000	250.000	250.000	250.000	250.000
% of overstayers identified	0	0	0	0,05	0,10	0,12	0,14	0,16	0,16	0,16
Cost of identification per person	0	0	0	4.500 €	4.500 €	4.500 €	4.500 €	4.500 €	4.500 €	4.500 €
Saved cost of not having to increase Imm. Enforcement Services (in million €) to identify more overstayers	***0***	***0***	***0***	***56,25 €***	***112,50 €***	***135,00 €***	***157,50 €***	***180,00 €***	***180,00 €***	***180,00 €***
Number of return decisions	0	0	0	250.000	250.000	250.000	250.000	250.000	250.000	250.000
% of decisions implemented	0	0	0	0,50	0,50	0,50	0,50	0,50	0,50	0,50
additional % of return decision implemented	0	0	0	0,04	0,08	0,13	0,18	0,23	0,28	0,33
Workload per return decision				20,00	20,00	20,00	20,00	20,00	20,00	20,00
Hourly cost				30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €
Saved cost on better execution of return decision	***0***	***0***	***0***	***6,00 €***	***12,00 €***	***19,50 €***	***27,00 €***	***34,50 €***	***42,00 €***	***49,50 €***
Benefit for Immigration Enforcement (in million €)	**0,0**	**0,0**	**0,0**	**66,9**	**129,3**	**159,5**	**189,7**	**219,9**	**227,6**	**235,3**
Total benefits	**0,00 €**	**0,00 €**	**0,00 €**	**16,24 €**	**207,21 €**	**340,37 €**	**458,63 €**	**559,69 €**	**581,00 €**	**602,86 €**

12. ANNEX 12: COST-BENEFIT ANALYSIS

12.1. Cost-Benefit of Preferred Solution

In this section the Smart Borders system is synonym for the EES preferred solution.

The cost-benefit analysis is produced using the results developed in previous annexes:

– "Annex 6 – Cost Model for Smart Borders system" contains the cost for the development and maintenance of the Smart Borders system, both the central and the national part. The model is based on cautious assumptions on cost components and does not take items of possible cost reductions into account, such as volume discounts on procured items. The model is also based on the assumption of 30 Member States in the Schengen area (both EU countries and associated countries) from the start.

– "Annex 10 – Implementation costs at National level" provides an estimate for the costs incurred within 30 Member States for the set-up of the system and in particular the investments in additional or renewed border crossing equipment.

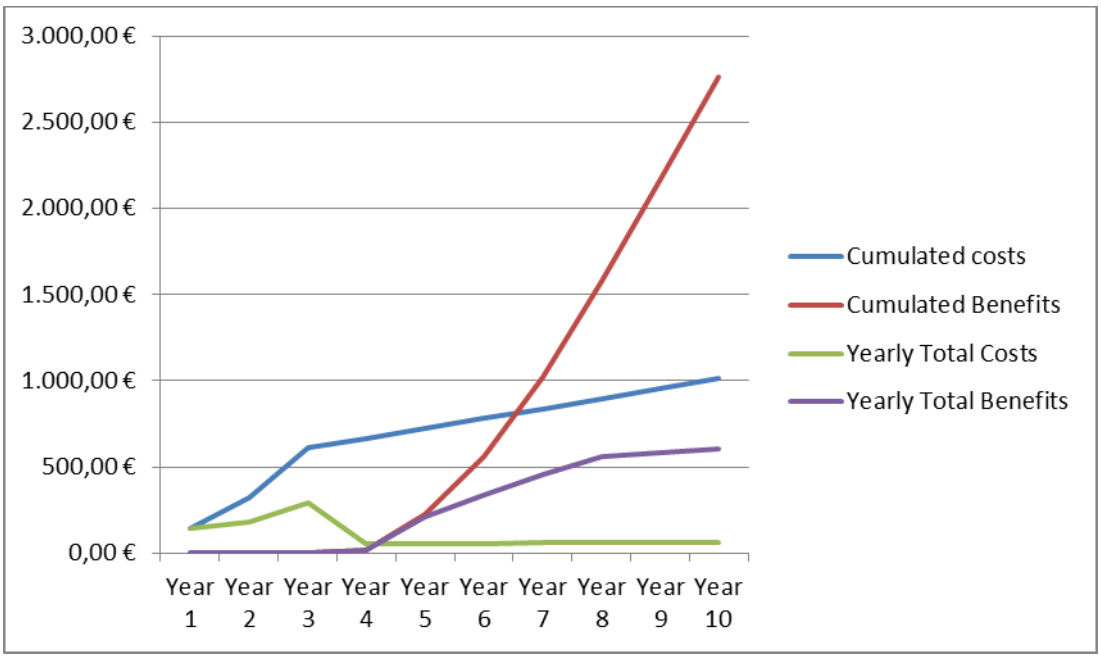
– "Annex 11 – Benefits of Smart Borders of preferred solution" estimates the benefits systematically using cautious values. The benefits are also computed for the number of third country nationals entering or leaving the current Schengen area, which is only 26 Member States as Bulgaria, Croatia, Cyprus and Romania are not part of the Schengen area at the moment of this computation (2015).

The summary of these computations is shown in the chart below (all figures in million €):

Cost-Benefit Estimation	Development year 1 2017	Development year 2 2018	Development year 3 2019	Operations Year 1 2020	Operations Year 2 2021	Operations Year 3 2022	Operations Year 4 2023	Operations Year 5 2024	Operations Year 6 2025	Operations Year 7 2026
	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Costs										
Development and Operations of Smart Borders		Part highlighted represents the €480,2 million of financial annex								
Central System					26,32	27,07	27,43	27,43	27,43	27,43
National systems					19,71	19,71	19,71	19,71	19,71	19,71
Total	112,65	115,60	206,52	45,47	46,03	46,78	47,14	47,14	47,14	47,14
Changes SIS II and VIS	0			0	0	0	0	0	0	0
Total Development and Operations of Smart Borders	**112,65**	**115,60**	**206,52**	**45,47**	**46,03**	**46,78**	**47,14**	**47,14**	**47,14**	**47,14**
Compliance costs MS (see Annex 10)	30	62	82,5	11	11	11	11	11	11	11
Total Costs	**142,65 €**	**177,60 €**	**289,02 €**	**56,47 €**	**57,03 €**	**57,78 €**	**58,14 €**	**58,14 €**	**58,14 €**	**58,14 €**
Cumulated Costs	**142,65 €**	**320,25 €**	**609,27 €**	**665,74 €**	**722,77 €**	**780,55 €**	**838,69 €**	**896,83 €**	**954,97 €**	**1.013,11 €**
Benefits										
Border crossing time benefit in million € - Traveller's benefit	**0**	**0**	**0**	**-7,60 €**	**82,37 €**	**164,30 €**	**236,77 €**	**298,28 €**	**310,22 €**	**322,62 €**
Benefit on Border Control Services (in million €) - Border guard's benefit	**0**	**0**	**0**	**-43,04 €**	**-4,47 €**	**16,58 €**	**32,16 €**	**41,50 €**	**43,16 €**	**44,89 €**
Impact for Immigration Enforcement										
Benefit for Immigration Enforcement (in million €)	**0,0**	**0,0**	**0,0**	**66,9**	**129,3**	**159,5**	**189,7**	**219,9**	**227,6**	**235,3**
Total benefits	**0,00 €**	**0,00 €**	**0,00 €**	**16,24 €**	**207,21 €**	**340,37 €**	**458,63 €**	**559,69 €**	**581,00 €**	**602,86 €**
Cumulated benefits	**0,00 €**	**0,00 €**	**0,00 €**	**16,24 €**	**223,45 €**	**563,82 €**	**1.022,45 €**	**1.582,14 €**	**2.163,14 €**	**2.766,00 €**
Benefits - Cost	-142,65 €	-177,60 €	-289,02 €	-40,23 €	150,18 €	282,59 €	400,49 €	501,55 €	522,86 €	544,72 €
Cumulative	-142,65 €	-320,25 €	-609,27 €	-649,50 €	-499,32 €	-216,73 €	183,76 €	685,31 €	1.208,17 €	1.752,89 €
Discounting value (rate 4%)	1	0,96	0,92	0,89	0,85	0,82	0,79	0,76	0,73	0,70
Net Present Value (when (cost-benefit) are taken over 1,2, ..n years)	**-142,65 €**	**-313,42 €**	**-580,63 €**	**-616,40 €**	**-488,03 €**	**-255,76 €**	**60,75 €**	**441,89 €**	**823,94 €**	**1.206,65 €**

Evolution of Costs and Benefits

The result of this computation is shown more explicitly in the chart below.



Graph of yearly and cumulated costs and
yearly and cumulated benefits for Smart Borders in million €

Yearly total costs are substantial at the beginning and reach a peak in year 3 as major investments need to be made before the beginning of operations. The line of cumulated costs has a steep slope over that period. Benefits being zero over that period of time, the cumulated benefits are also zero.

Once the system starts to be in operation, benefits start to accumulate. As the benefit computation model assumes a progressive uptake of potential benefits that Smart Borders creates (see line of Yearly Total Benefits), the slope of the yearly benefits is modest and becomes nearly flat from year 8 onwards. The benefits are however substantial and explain why the cumulated benefits line increases quickly and crosses the line of cumulated costs. Once the system is in operation, the yearly total costs almost stagnate (see line of Yearly Total Costs). The cumulated costs still grow but at slower pace as compared to years 1 to 3 (the slope flattens).

Net Present Value

Based on the costs estimated for 30 Member States and the benefits for only 26 Member States, the **net present value** at the beginning of the project has been computed for future costs and benefits using a discount rate of 4%.

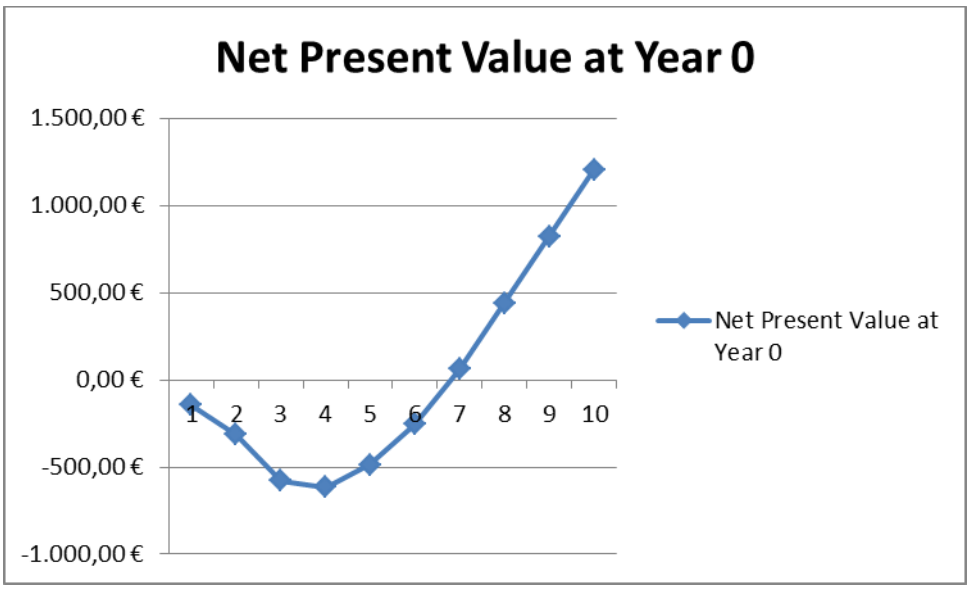


Chart showing the Net Present Value (in million €) after 1, 2... N years

The net present value decreases when costs and (zero) benefits of the first three years are discounted to the beginning of the project. As benefits outweigh more and more costs over the next years, the net present value at the beginning of the project becomes positive after four years of operations.

12.2. Preferred Solution vs Building no Smart Borders system

The scenario of the preferred solution has been compared with the alternative scenario in which the Smart Borders system was not introduced.

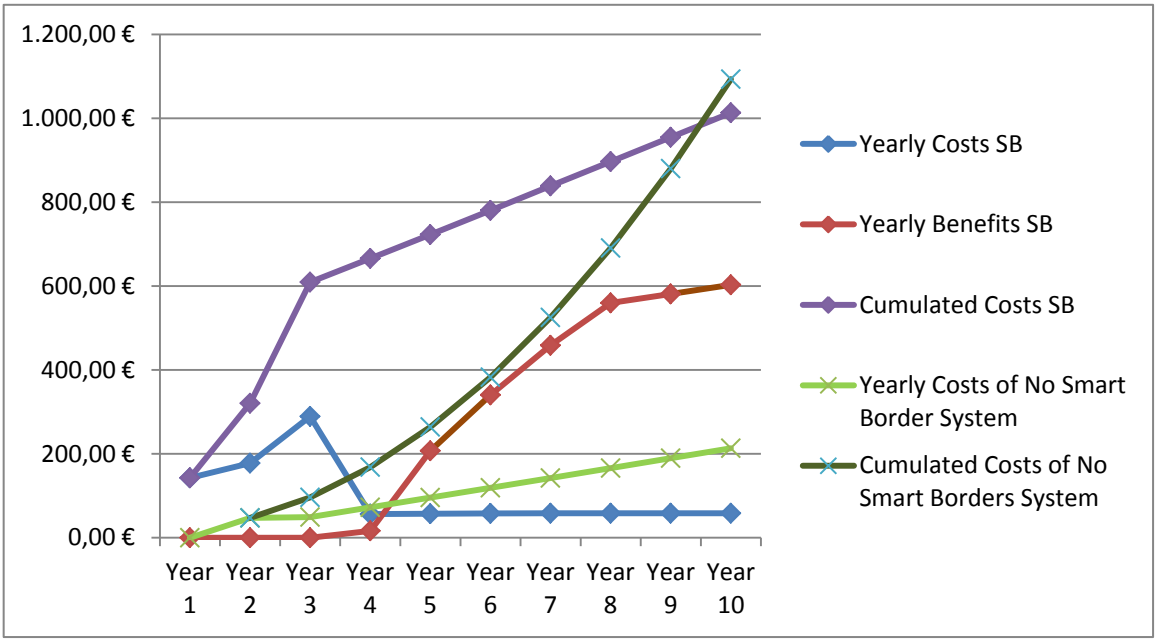
In this alternative scenario, Member States would incur a series of costs in order to:

– Keep the duration of border crossings unchanged. Considering that the number of border crossings increases, the number of border guards in first line would have to increase in the same proportion.
  The recruitment of more border guards induces a recruitment cost and an equipment cost.

– Achieve an equal amount of return decisions from year 4 (first year of operations) as in the situation where the Smart Borders system is implemented. In order to do so, an increased number of staff in Immigration Enforcement services would have to be recruited with their corresponding associated costs.

The benefit of not building Smart Borders compared to the current situation is by definition zero.

The results of this computation are shown on the graph below and compared with the situation where Smart Borders is built:



Horizontal axis as years after Smart Borders project start – Vertical axis in million €
Graph compares yearly costs and benefits and cumulated costs and benefits
when Smart Borders system is built with the situation
where no Smart Borders system would be built but same operational results are expected

The picture shows:

– That the **yearly costs** with the Smart Borders system ("Yearly Costs SB") remains about half the yearly costs without Smart Borders ("Yearly Costs of No Smart Border System") for the years after the system is in operations (i.e. from year 5 onwards).

– The development and implementation of Smart Border is a cost-intensive operation. This is shown by the fact that the line "Cumulated Costs with SB" only becomes inferior to "Cumulated Costs of No Smart Borders System" at the end of year 9: the high initial cost of introducing SB is compensated over time by a lower yearly operational cost.

– The **yearly benefits** of the Smart Borders system are significantly higher than without assuming resources are provided to deliver the same results. The reason is that the Smart Borders system provides efficiency gains to travellers, border guards and immigration enforcement services ("less workload for more results"). Without Smart Borders there is no reduced dwelling time for travellers, no reduced workload for border guards when traveller use self-service kiosks and no increased number of return decisions for equal staff numbers.

13. ANNEX 13: IMPACT ASSESSMENT ON FUNDAMENTAL RIGHTS

The objective of this annex is to describe in detail the assessment of the impact on Fundamental Rights of the "preferred solution" of the proposal for a "Regulation establishing an EU Entry-Exit System and for a Regulation amending the Schengen Border Code.

13.1. Why is this impact assessment necessary

An Entry Exit System (EES) would, due to the personal data involved, in particular have an impact on Fundamental Rights and particularly on the right to the protection of personal data. The right to protection of personal data is established by Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty of Functioning of the European Union. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter and by Article 8 of the European Convention on Human Rights (ECHR). This is further reflected by Article 1(1) of Directive 95/46/EC which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

Therefore, the impact assessment on Fundamental Rights of the proposal is necessary because the proposed regulation for an EES will result in processing the following personal data:

(1) the identity as recorded in the biographical page of the passport to be copied for all visa-exempt third country nationals (TCN-VE), including two biometric identifiers (four fingerprints and the facial image),

(2) the identity of all visa-required third country nationals (TCN-VH) stored in VIS being used to identify the person and a facial image being taken,

(3) the place, date and authorising authority to be recorded and stored at the entry into the Schengen area of each third country national,

(4) the place and date to be recorded at exit from the Schengen area of each third country national,

The data listed above will be stored for a period of five years counting from the date of the last exit record.

The EES record would contain:

(5) Five individual file data: first name, surname, date of birth, nationality or nationalities and gender. These data will all be taken from the Machine Readable Zone or the chip of the travel document;

(6) Two biometric identifiers: the four fingerprints (FP) and the facial image (FI);

(7) Four data elements from the travel document: document number, document type, document country code and expiry date. The data elements for documenting the refusals of entry will also be recorded as they are a key border crossing information;

(8) Four visa-related data in case of visa-required third-country nationals (TCN): visa sticker number, visa expiry date, number of authorised entries and authorised period of stay;

(9) Five data elements for registering stay changes: the revised expiry data of the authorisation of stay, the date of change of limit of stay, the place of change of limit of stay and the ground for change or revocation;

(10) Five date elements for each entry/exit record: date and time of entry, entry authorising authority, entry BCP, date and time of exit and exit BCP;

(11) Two data elements for each RTP scheme the traveller has been entitled to: the unique RTP reference number (this is assumed also identify the RT scheme) and the RTP status information.

There are in total 27 data elements as compared to the 36 data elements of the 2013 proposal.

The items above demonstrate that the EES will record and store a small amount of personal data including biometrics from a large amount of people (order of magnitude of 50 million people per year) as well as their entry and exit record(s) stored over the duration of the retention period.

13.2. Approach

The approach followed covers an impact assessment on all rights that are part of the Charter of Fundamental Rights (the Charter), focusing on Articles 7 and 8 as the impact on these rights is the most obvious.

Under Article 7 of the Charter: "*Everyone has the right to respect for his or her private and family life, home and communications*".

This article must be read in conjunction with Article 52(1). Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be (1) provided for by law, (2) respect their essence and, (3) subject to the principle of proportionality, (4) limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[5]

Concerning the principle of proportionality three elements must therefore be assessed in combination:

(1) the measure must be appropriate (suitable),

(2) the measure must be necessary (requisite), which includes an assessment to determine whether there is no less intrusive alternative,

(3) the measure must be proportionate.

Article 8 is a proactive horizontal right to protection that is not limited to interferences by the State. It gives individuals the right that their personal data can only be processed if the requirements set out in paragraphs 2 and 3 of Article 8 are met:

[5] See Judgment of the Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000, paragraph 65.

(4) the data is processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law,

(5) transparency is ensured by giving the individuals rights to access and correction,

(6) control by an independent authority is ensured.

The sequence of items addressed in this Impact Assessment essentially follows the presentation done by the EDPS (European Data Protection Supervisor) during the workshop with DG HOME on 20 March 2015 as part of the consultations in preparation of the modified legal proposal. In this approach, the way the impact of measures on Articles 7 and 8 of the Charter of Fundamental Rights is assessed, reflects the European Court of Justice ruling on the Data retention directive on telecommunication data.

The assessment is first made **without assuming access to data by law enforcement authorities** (see point 14.3) and then separately **when this access is granted** (see point 14.4).

13.3. Impact Assessment of the preferred solution

13.3.1. Legal ground of the data processing

The regulation for an Entry-Exit System provides the legal ground of the data processing including the collection, storage, use and deletion of the data enumerated under section 13.1. The EES regulation has been developed in full respect of the *privacy by design*[6] principles.

13.3.2. Respect of the essence of the right to privacy, objectives of general interest and proportionality

So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by the EES Regulation constitutes an interference with those rights, it is not such as to adversely affect the essence of those rights given that the Regulation only permits the use of the EES data to officials from competent authorities for border and migration control.

Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because the EES Regulation provides, in relation to data protection and data security, that certain principles of data protection and data security must be respected by Member States. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted to amend data which it has introduced into the EES, by correcting or deleting such data in accordance with the EES Regulation.

From the above the conclusion is that the "essence" to the right of privacy is not altered: the EES does not record an amount of data that would correspond to a permanent tracing of traveller movements. The frequency of the recording is also low as it only happens at entry and exit of the Schengen area and no intra-Schengen movements are included.

The proposed regulation pursues two objectives of general interest:

[6] Privacy by design means embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a proposed purpose and granting data access only to those entities that ‘need to know.’

(1) Improve the management of external borders.

(2) Reduce irregular migration, by addressing the phenomenon of overstaying.

Improved border management pursues increased effectiveness and efficiency of border controls at the external borders. Effectiveness in border management is achieved if it facilitates the border crossing of bona fide travellers whilst at the same time prevents that "non-bona fide" travellers enter the Schengen area or are apprehended at exit. Efficiency in border management is achieved when the increase of border crossings does not require a similar increase of border guards. The objective of improved border management means that the level of detail is adapted according to an individual risk assessment performed by the border guard. But such a risk assessment is based, like it is the case today, on identifying the traveller, as a starting point, and on information about the traveller's past behaviour as regards immigration rules.

The second objective is achieved by the EES computing the remaining duration of stay at entry and verifying the overstay status at exit. The EES provides the Schengen area with the tool that systematically verifies whether the basic rule on the duration of stay and applicable to all third-country nationals entering Schengen for a short stay is respected.

The principle of proportionality is met for the following reasons:

– The scope of the measure addresses only the third-country nationals entering the Schengen area for a short stay. The measure does not include third-country nationals with long-stay visas or residence permits. It also excludes third-country nationals crossing the land borders of the Schengen area with a Local Border Traffic permit. It further excludes EU nationals and persons enjoying the right of free movement. Although the group of impacted persons is a large group it represents roughly less than 1/3 of border crossings and less than the same proportion of persons crossing the border as a significant proportion of them travel frequently to the Schengen area.

– A further narrowing of the scope of persons whose personal data would be collected is not possible without introducing discrimination on the basis of nationality. Currently identified overstayers stem both from visa-required and visa-exempt countries but with numbers varying according to a mix of circumstances in their home country and evolving over time. Further, the scope of persons strictly corresponds to the one on which the rule on duration of short stay applies according to the Schengen Border Code.

– The data that are recorded are all justified by the need to uniquely identify the person and to establish compliance with the duration of stay. There are no data recorded for other purposes and that would infringe the privacy of the person like indications on who is accompanied by whom or the means of transport used. These examples of data are currently recorded by national occurrences of entry-exit systems serving law enforcement purposes but are excluded from EES.

– The identification data are copied from the travel document and the biometrics from the traveller. The entry and exit data are taken at the moment of the border crossing. As a consequence, there are no data collected without the traveller knowing about, nor on the basis of traveller declarations or subjective appreciation of border guards.

– Although it does not diminish the need for the current privacy Impact Assessment, it is a reassuring element for the traveller to know that authorities that will have access

to EES data will not see more information about him/her than is currently the case when handing over his/her travel document.

The principle of proportionality is respected as the data stored strictly meet the legitimate objectives pursued by the Regulation listed above and as the group of persons to whom it applies strictly corresponds to the ones affected by the applicable rule on duration of short stay.

13.3.3. Precision of the measures

The proposed measure is extremely precise both in terms of the group of persons whose personal data will be recorded, the data themselves, the processing of data and the exchange of data.

The group of persons whose data will be recorded are third country nationals who enter the Schengen area for a short stay (defined under the Schengen Border Code as "no more than 90 days within any 180 days period"). It therefore excludes third-country nationals entering the Schengen area with a long-stay visa, the residence permit holders (so third country nationals living in a Schengen country), residence card holders (these are the persons enjoying the right of free movement) and the persons crossing the border on the basis of a Local Border Traffic Permit.

The data themselves are defined up to the level of the data element. Each data element is itself very accurately specified either in the regulation, in the legislation referred to (the VIS Regulation), or by internationally recognised standards (the definition of the contents of ICAO compliant travel documents).

The processing of the data is also extremely precise:

– For visa-exempt third country nationals, data are recorded at the border crossing point of entry into the Schengen area and at the border crossing point of exit.

– For visa-required third country nationals, identification data from the visa-application are retrieved and referenced in the Entry-Exit system. Entry and exit data are recorded in the same circumstances as for visa-exempt third country nationals.

– Consultation of personal data is only possible by officials from competent authorities for migration control or enforcement.

– When other authorities or private operators (this is the case for carriers) need to ascertain that a third-country national is lawfully staying within the Schengen area, the solution retained is that a "YES/NO" answer is given by a web-site which accesses a report from the Entry-Exit database. With this mechanism the privacy of travellers is increased compared to the current situation. Currently travellers hand over their passport containing the history of all their entries and exits to any request while with the proposed solution the passport data will only allow receiving the confirmation that the person is staying lawfully in the Schengen area.

– The EES will either compute durations of stay, flag cases of overstay and produce statistics. Statistics can only be produced for specific stakeholders (Member States competent authorities, European Commission and Frontex) and does not require a direct access to the individual data. Production of statistics contains also a safeguard mechanism that avoids statistics to be produced for such small numbers of affected

persons that de facto individual persons can easily be identified (example a report on the number of persons who overstayed in a narrowly defined time period coming from a third country with a very small number of citizens coming to the Schengen area may be so small that it is clear who these persons could be). This last provision is referred to in the legal proposal by the fact that the development of the system will take security of the system and protection of its data into account.

– The conditions for correcting and/or deleting data from EES are also defined in the regulation. It can be noted that the correction of data either by competent authorities or on the request of the data subjects takes into account the feed-back received from travellers during the survey carried out by the Fundamental Rights Agency. It appeared from this survey that travellers were mainly concerned on how potentially wrongly recorded data could be corrected.
  Further, the conditions for deleting data are also specified and address cases where third country nationals request asylum or refugee status after having entered the Schengen area for a short visit as well as the cases where a traveller falls under the conditions where entry-exit data are not recorded (example: the third country national obtains a long stay visa or becomes the family member of an EU citizen).
  The deletion of all data (identification data and entry-exit records) becomes automatic and non-reversible for all third-country nationals whose last exit date reaches the data retention period. For third-country nationals who are still identified as overstayers at the end of the data retention period in EES, data are removed from EES, and handed over to each Member State for possible introduction into SIS. From that date onwards, these personal data are subject to the data retention provisions for SIS data.

– The processing of data is performed by eu-LISA, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. As such, the data are stored in the EU and remain submitted to EU legislation on data protection.

– The exchange of EES with third countries or with private companies is excluded in the regulation.

13.3.4. Purpose limitation

The objectives pursued for collecting the personal data, as listed under section 13.3.2 above, are extremely clear:

(1) Improve the management of external borders.

(2) Reduce irregular migration, by addressing the phenomenon of overstaying.

Improved border management pursues increased effectiveness and efficiency of border controls at the external borders. The effectiveness of border management can only be increased by differentiating the intensity of the thorough control required by the Schengen Border Code according to an assessment of individual migration risk. As an example, the migration risk for a visa-exempt traveller who was refused entry a previous time is different than for another traveller who visits relatives every year during holidays. This migration risk, which is the only risk addressed by this proposed regulation, cannot be assessed quickly and clearly enough when the border guard needs to read Schengen stamps among the stamps of other destinations. In addition the traveller is left the opportunity to hide past events (like a refusal of entry) simply by changing passport. It is abnormal that up to now the appreciation of migration risk happened exclusively on the

basis of the information contained in a travel document carried by the traveller with no equivalent information owned by the authorities in charge of migration. The traveller is up to now left with the decision of changing passport (which can be easily done by pretending a loss or voluntarily destroying it) or by using another one in the case of persons having more than one passport, from the same or from different countries, which is not uncommon.

The second objective is achieved by the EES computing the remaining duration of stay at entry and verifying the overstay status at exit. The EES provides the Schengen area with the tool that systematically verifies whether the basic rule on the duration of stay and applicable to all third-country nationals entering Schengen for a short stay is respected.

The first objective leads to store entry and exit records over a sufficiently long retention period. By analogy with the current de facto average retention period of information in a passport, the retention period is five years. The second objective does not add additional requirements as regards the data to be collected.

Both objectives however require establishing the identity of the traveller first. If this would not be done, entries and exits could be wrongly attributed to homonyms after a passport changed or when multiple passports are used by a same person. Biometrics are used in order to avoid an unacceptable level of inaccuracy in establishing the identity.

The only further processing of data occurs for overstayers at the end of the date retention period. Five years after the last entry date, which by definition is not matched with an exit date, personal data are removed from EES and on Member State's decision included in SIS. This is the only further processing of a percentage-wise small amount of the EES data. This further processing is compatible with the original purpose as it remains an immigration control measure. By storing these data into SIS, overstayers are not criminalised but continue to be registered in order to remain identifiable and to be removed from the Schengen territory and not be authorised to enter again.

13.3.5. Data processing is adequate, relevant and not excessive

The proposed data processing consists in recording the entries and exits of all third country nationals entering Schengen for a short stay.

The data that are proposed to be recorded can be split into three main categories: the data that establish the identity of the person including his biometrics, the data that establishes the entitlements to stay (like the availability of a visa or the extensions of duration of stay), the successive entry and exit dates that are the basis for computing the authorised duration of stay.

Adequacy and relevance for improved border management

The first objective pursued is improved border management. The problem at stake is that third country nationals represent 200 million border crossings in 2014 and an estimated 300 million border crossings in 2025. At the same time the number of border guards is not expected to grow within the same proportions. The way this can be done is by automating controls and by focusing the depth of the controls on the travellers representing a migration or security risk.

Automating border controls of third-country nationals for a short stay is possible with current technology. The border control schematically involves three steps: establishing

the identity of the person, verifying whether entry (or exit) conditions are fulfilled, authorising the entry for a specific duration of stay. Current technology improves the precision and speeds up the identity verification and can help determine the authorised duration of stay. Verifying the entry (or exit) conditions is currently done by asking a set of questions. This questioning part can be targeted according to the migration risk assessed by looking into the past history of entries and exits, and relevant information about the country of origin. The security risk is addressed by the systematic control vs SIS and national databases.

The envisaged data processing allows recording identities, linking a history of entry and exit movements and automating the computation of the authorised duration of stay. The only part that is not automated is the questioning part which can be prepared using automated means or can be replaced by a pre-vetting in a nationally defined trusted travellers scheme.

The proposed data collection is not to reduce necessarily the duration of the border crossing for the traveller as this duration is already very low but to decrease the work effort for border guards so that their number can increase less quickly than the number of border crossings. Both the technical study and the pilot have demonstrated the relevance of the proposed data collection provided the enrolment of travellers in EES (in practice this enrolment is only required for visa-exempt travellers) does not need to be repeated frequently as this is the only process step taking longer than the current one. Improved border management therefore relies on a sufficiently long data retention period of the data set containing 27 data elements described earlier.

Adequacy and relevance in reducing overstay

In order to assess whether the proposed measure is not excessive, the magnitude of the existing problem needs to be evoked. The current way of doing border controls in accordance with the Schengen Border code has not prevented that an estimated 1,9 to 3,8 million persons[7] are irregular migrants. This amount is assumed to increase by another 250.000 persons on a yearly basis. The majority of these irregular migrants have not smuggled into Europe but have simply used regular migration paths and overstayed. The recent migration waves in Europe via the Mediterranean Sea and the Balkans essentially concern refugees fleeing war circumstances and are different from the overstayers mentioned before.

The EU has developed a return policy to curb the volume of overstayers but this policy is hampered by the fact that the date and place of entry into the Schengen area are unknown. As the return needs to be done towards the country of origin or from where the overstayer came from the current policy reaches its goal for only 50% of returns as the required information is currently not recorded. Only visa-required travellers can be identified vs VIS on the basis of their fingerprints, but even for these travellers the place and date of entry are not recorded.

When the proposed data are collected for all travellers concerned by the measure, migration authorities are given the tools to get a grasp of the situation. Authorities will start to be able to identify the overstayers, estimate their number and where they come from. When overstayers are "picked up on the street" their identity can be established and

[7] Estimates from the Clandestino project, an EU-sponsored project implemented by the International Centre for Migration Policy Development. More precise and updated figures are not available.

a return successfully executed. The data processing is therefore adequate, relevant and proportionate with the migration problem at stake.

The relevance of the data collection is objected by stating that as the EES does not locate overstayers (no addresses are recorded), authorities will only be able to identify overstayers but not apprehend them. The argument is not very relevant as the problem today is not finding overstayers but establishing their identity as they often destroy their travel document and/or try to acquire EU documents to secure their situation. Finding overstayers is done by investigating the places where they seek jobs and not by collecting addresses.

A second objection to the relevance of the data collection is that Europe needs more workers with its declining demography and that overstayers should therefore not be tracked but welcomed. The argument is not relevant either because the EU has opted for a chosen migration and not for having to accept overstayers who impose their presence. Treating overstayers the same way as persons following regular migration schemes means that a premium is given to irregular migration and completely undermines the chances of success of controlled migration.

Relevance of biometric data

At the kernel of the EES identity file are the biometrics. The biometrics are only a tool for establishing the identity of a person accurately. The following question needs to be answered: why biometrics need to be stored on top of the biographical information of the traveller? The reasoning could be made that recording entries and exits of third country nationals is adequate, relevant and not excessive for the objectives pursued and there is no need for storing the biometric identifiers.

The biometric identifiers of the preferred solution are the facial image and four fingerprints at enrolment. These identifiers are used in three situations:

– Situation 1: verification at the border. Verifying that the identity on a passport matches the identity in the EES so that entries and exits are recorded for the right person. For this purpose one identifier like the facial image is enough or one fingerprint from the set of four recorded.

– Situation 2: identification at the border. Identifying whether a person was already recorded so that entries and exits are not allocated to a new individual file while the person was already enrolled. For this purpose the identification is conducted using the facial image and the four fingerprints to obtain a sufficient accuracy.

– Situation 3: identifying a non-documented traveller. This is the situation where the identity of a person (often an overstayer) needs to be established potentially in the absence of any travel document. Like in situation 2, the identification is conducted using the facial image and the four fingerprints.

There are three reasons why only biographical information would not be sufficient for the first situation which is the situation most often encountered:

– There is a high proportion of homonyms among the names of third country nationals. The only strong identifier[8] is the combination of passport number and issuing country.

[8] A strong identifier in IT means an identifier that is unique and stable. In a personnel database, the strong identifier is the personnel number but not the first and last name as both can have homonyms.

This identifier is however not stable over time as the passport can be changed following expiry, loss, theft, or involuntary destruction to cite the most common cases. The proportion of homonyms is much higher among the names of third country nationals[9] than of citizens of Schengen countries which makes that relying solely on name matching or biographical data is very error prone. The biometric data provide the unsurpassed benefit of linking in a stable and reliable manner an identity to a same physical person.

– The situation of homonyms is worse as names that are originally not spelled in Latin alphabet are transliterated. This transliteration maps differently spelled names potentially to a same transliterated name. However, the transliteration rules are not necessarily stable over time and are not consistently applied, which makes that successive passports of a same person do not spell a name in exactly the same way. Linking entry/exit records on the basis of first and last name as well as any other key based on this appears even more error prone.

– Persons do not necessarily keep the same name. Only a limited number of countries try to consider the name as a strong identifier. In many countries the name changes according to the marital status and to other events in life. For perfectly lawful reasons, a same person can therefore appear at two successive moments with different names. Again, name matching appears to be very error prone.

The situation 2, where a person has different travel documents for legal reasons (example: a significant minority of persons has two nationalities or two passports for convenience reasons), needs to be detected. Otherwise, a same person could stay indefinitely in the Schengen area by being enrolled twice but with a different passport and alternating its use in order never to exceed the duration of stay. Given that not all cases would be detected by only relying on name searches a biometric identification is required.

The situation 3, where a person has no travel document, is the most obvious case where only biometric identifiers can be used to search the EES database. The experience of VIS has demonstrated the importance of this capability as on a yearly basis about 14.400 (about 1.200 per month)[10] are done and follow an upward trend as more biometrics are available now than before.

It can be noted that at the level of a single EU Member State, citizens are not identified by means of their first and last name but by means of a so-called "concatenated key" composed of "first names (plural), last name, date of birth (day/month/year) and place of birth". However, even in this case the risk of confusing persons was still deemed too high and a unique national identifier was introduced (e.g. a social security number or a national register number). There is no such universal identifier available and the "concatenated" key used at the level of an EU Member State would not work for third-country nationals as their passports do not contain the place of birth and the date of birth is often simply a year.

[9] As an example there are ten names shared by 100 million Chinese citizens. A similar situation exists in other Asian countries.

[10] Obtained from regular statistics on the use of VIS produced by eu-LISA. Values used refer to March 2015.

As a conclusion, biometric identifiers are adequate and relevant for identifying travellers accurately. They therefore reduce significantly the risk of confusion between identities as there is no other universal unique and stable identifier of individuals.

Why these biometric identifiers?

The minimum set of biometric identifiers (i.e. the facial image and 4 fingerprints at enrolment) has been chosen for the intended use in the three situations mentioned above (i.e. verification at the border, identification at the border, documenting undocumented persons). This choice represents the minimum set of identifiers that can establish identity with a high accuracy given the number of travellers who will be recorded (i.e. the 'lighter'/'smaller' biometric identifiers necessary and sufficient for the specified purposes of identification of third country nationals crossing the Schengen area external border). The proposal will also foresee that verification can be done on the basis of the facial image only. The other potential options would consist in recording 8 or 10 fingerprints in addition to the facial image. Capturing 8 or 10 fingerprints at all borders increases precision for identification but only marginally while, at the same time, it becomes operationally very burdensome and it has a significant negative impact on waiting times for travellers.

13.3.6. Proportionality test

The questions to be answered under this heading are:

Need for an additional border control measure

The question raised is whether existing data collections do not or could not fit the purposes pursued by the EES. It is different from the technical question whether the EES needs to be built as an extension of an existing system (the VIS is usually cited) or by reusing components of another one. What matters here is whether a new (important) collection of personal data needs to be created on top of the existing ones.

There are currently three large-scale IT systems in operation in the area of Justice and Home affairs. The table below summarises their purpose, data content and data retention period.

Instrument	Purpose(s)	Personal data coverage	Data retention
Visa Information System (VIS)	To help implement a common visa policy and prevent threats to internal security.	Visa applications, fingerprints, photographs, related visa decisions and links between related applications.	5 years.

Instrument	Purpose(s)	Personal data coverage	Data retention
Schengen Information System (2nd generation) **(SIS)**	To ensure a high level of security in the area of freedom, security and justice and facilitate the movement of persons using information communicated via this system.	The data categories in SIS plus fingerprints and photographs, copies of European Arrest Warrant, misused identity alerts and links between alerts. SIS alerts relate to several different groups of persons.	Personal data entered in SIS for the purpose of tracing persons may be kept only for the time required to meet the purpose for which they were supplied, and no longer than three years. Data on persons subject to exceptional monitoring on account of the threat they pose to public or national security must be deleted after one year.
EURODAC	To assist in determining which Member State should assess an asylum application.	Fingerprint data, sex, the place and date of the application for asylum, the reference number used by the Member State of origin and the date on which the fingerprints were taken, transmitted and entered in the system.	10 years for asylum-seekers' fingerprints; 2 years for those third country nationals apprehended in connection with the irregular crossing of an external border.

Visa Information System (VIS)

The main purpose of the Visa Information System (VIS) is to permit the verification of the visa application history and to verify whether the person presenting the visa at the border is the same person to whom the visa has been issued at entry.

It concerns only those third-country nationals who are required to hold a visa. The VIS was not developed to keep track of entries and exits of third-country nationals nor is it meant to allow checking whether a person, after entering the EU legally, has or has not complied with the authorised stay according to the visa. Therefore the possibility of including entry/exit functionality in the VIS itself and the storage related to non-visa holders in the VIS can be discarded.

However, there would be major technical and functional links between the VIS and the EES. Besides the same technical features and a common matching functionality, VIS is the repository of the biometric identifiers of visa holders who will be registered in the EES. The fingerprints of the visa holders would not be stored in the EES as they already exist in the VIS. The EES would re-use the visa holder fingerprints already captured for the benefits of VIS, without duplicating the effort and avoid storing the fingerprints of visa holders twice.

Schengen Information System

The Schengen Information System (SIS) provides access to alerts on persons and objects to a large set of authorities including migration and border control, law enforcement and judicial authtorities.

The main categories of alerts are:

– Persons wanted for arrest for extradition purposes;
– Third-country nationals to be refused entry to the Schengen territory;
– Missing persons (children and adults);
– Witnesses and persons required to appear before the judicial authorities in connection with criminal proceedings;
– Persons or vehicles to be put under discreet surveillance or for specific checks;
– Certain categories of objects (e.g. stolen identity cards, vehicles, firearms, bank notes).

The SIS operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system. The SIS enables authorities to check persons and objects both at external borders and within the territory of the Schengen States. The SIS provides law enforcement authorities with information on why a certain individual is wanted, what action is to be taken and whether the person is presumed violent and armed.

However, as the information contained in the SIS is only sufficient for the authorities on the ground to take the correct initial actions, it is necessary for the Member States to be able to exchange supplementary information, either on a bilateral or multilateral basis, as required for implementing certain provisions of the Schengen Convention, and to ensure full application of Title IV of the Schengen Convention for the SIS as a whole.

The description above evidences that the SIS is not designed to record entry and exit data and compute durations of stay.

Eurodac

Eurodac is a fingerprint database that stores and compares the fingerprints of asylum applicants and irregular immigrants and which allows Member States to identify the State responsible for examining an asylum application in accordance with the Dublin II regulation. The Eurodac central unit operates a central database comparing fingerprints, an automated fingerprint identification system (AFIS) and a secure communication system for data transmission from and towards the national units (National Access Points) in Member States.

Neither the purpose nor the type of data Eurodac contains come even close to the objectives pursued by EES. On the contrary, it is when a person entered the Schengen area for a short stay and subsequently requests asylum that Eurodac can be used to check whether the same person already applied for asylum elsewhere.

Advanced Passenger Information and Passenger Name Record

For the sake of completion, and although these are not large-scale systems, they belong to categories of data to which the competent authorities potentially have access to.

Information collected on travellers, via Advanced Passenger Information (API) and via Passenger Name Record (PNR), applies to air and sea travel only for API data and to air travel only for PNR data: there is no information collected for crossing of land borders by individual means (personal car, (motor)bike, etc.) or by train. It is therefore not directly relevant for the EES. In addition, as these data are normally collected from airlines, travel agencies or entered by the traveller himself, the quality of the data is inferior to the data that would be collected from the travel documents at border control.

Conclusion. The investigation of the existing data collections concludes that none of the existing systems meets the purpose and contains data that correspond with EES at the exception of the VIS. The VIS contains identification data including biometrics for visa-required travellers but contains no data on visa-exempt travellers. The regulation therefore proposes for visa-required travellers to re-use the identification data from VIS and add their entry/exit records in EES, and for visa-exempt travellers to record both the identification data and the entry/exit data in EES. SIS and Eurodac have a completely different purpose and functionality than EES.

Least privacy-intrusive measure

The question whether there would be a less privacy intrusive measure is understood as answering two sub-questions: (1) is there a way for the number of travellers whose personal data are recorded to be reduced and (2) is there a way where less data could be collected from each traveller.

The number of travellers whose personal data are recorded corresponds strictly to the span of application of the Schengen Borders Code. The EES regulation does not modify the nature of the checks of the SBC but changes how they are done. The data collection is therefore also organised at the level where the SBC is applied: the whole Schengen area and not the constituent countries.

The amount of data collected for each traveller has been kept for the minimum. The description of the different data elements stored in EES (see section 13.1) and of the processing of data (see section 1.3.3) show that all data included have a justification and that less data would not allow to pursue the two objectives for the regulation (improved border management and reduce irregular migration). The biometric identifiers of the preferred solution are also the minimum set of biometrics that provide the accuracy required for linking entry/exit data to a personal file for the three situations (verification at the border, identification at the border, identification of non-documented person) where EES would be used.

Proportionality

It is the assessment of proportionality that led the European Court of Justice (ECJ) to annul Directive 2006/24 as the Court otherwise considered that the directive did not affect the essence of the right to private live and pursued objectives of general interest.

Compliance with the principle of proportionality has already been addressed to some extent in section 13.3.2 above.

Differentiation, limitation or exception in data collected.

As indicated in section 13.3.2 above, the measure addresses only the third-country nationals entering the Schengen area for a short stay as these are all submitted to the

same border control as per the Schengen Borders Code which is not changed on the substance.

The measure contains exceptions on the data collected as it does not include third-country nationals with long-stay visas or residence permits. It also excludes third-country nationals crossing the land borders of the Schengen area with a Local Border Traffic permit. It further excludes EU nationals and persons enjoying the right of free movement.

The result of the measure is that for visa-required travellers no additional personal data will be collected than already required under the VIS regulation but that entry and exit records will be stored per traveller over the duration of the data retention period. For visa-exempt travellers the result will be that personal identifiers will be collected as well the individual entry and exit records over the duration of the data retention period

The scope of persons whose personal data are collected as well as the data themselves correspond to the objectives pursued. The first objective of improving border control applies as well to the border control of visa-exempt and visa-required travellers. This is not the largest group of travellers but the one that represents the highest workload for border guards and where current methods for recording entries and exits (i.e. use of manual stamping) prevent any form of automation. Improved border controls need to rely on the result of past controls and on the improved accuracy of the identification of the traveller. The second objective of reducing irregular migration and overstay in particular concurs with the first objective on the data to be collected but requires the process of EES to calculate automatically the remaining duration of stay.

Link with specific migration objectives

The measure addresses under its second objective a specific migration objective of reducing irregular migration.

Conditions of access to data

Access is given to the data stored in the EES only for specified, explicit and legitimate purposes. The regulation provides that the authorities who will have access to the EES have to be designated for a specific limited purpose. The regulation can rely for this aspect on the VIS regulation which implemented the same approach.

Access for consulting the data is reserved exclusively to duly authorised staff of the authorities of each Member State who are competent for the specific purposes foreseen in the EES. Such access is limited to the extent to which the data are required for the performance of the tasks in accordance with these purposes.

The use of process accelerators

Concerning the use of process accelerators foreseen in the impact assessment, no additional information would be collected as there is no registered traveller's status and the facilitation is based on information already registered into the EES.

Furthermore, the use of modern IT systems, ABC gates and self-service kiosks at border controls can be perceived as less prone to discrimination as compared to checks performed by human beings. The prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21) could consequently be

positively impacted by the introduction of the EES. This question has been addressed by the Fundamental Right Agency survey (see Annex 15). The results of the survey showed that there is a widely held view that automated systems could cause less discrimination (e.g. on the basis of race or ethnicity) compared to checks carried out in person by border guards.

Data retention period

The main criterion used for the data retention period is that officials dealing with migration matters should have the same visibility on the travel history as it is currently the case when scrutinising the entry/exit stamps contained in a passport.

The majority of current passports have a validity period of ten years and there is usually the requirement that passports remain valid six months beyond the date of return. On average, a passport at the moment of its inspection by an authority contains a history of previous travels ranging between zero (a brand new passport) and nine and a half year (a passport close to the end of its validity). Given the large number of passports, the average situation is that the passport contains five years of entry/exit stamps. Hence the retention period is five years for all travellers.

The relevance of this data retention period is further confirmed by the fact that in the case of visa-required travellers the visa application data are kept for five years after expiry of the visa. The entry and exit data can be considered as the complementary information on how this visa was used and thus it is logic that the data retention period of EES and VIS data would be aligned. The validity of multiple-entry visas (MEV's) is also five years. For assessing the renewal of MEV's the consular officer currently examines the Schengen entry and exit stamps in the passports. With EES these entry and exit stamps of the Schengen area would no longer exist and hence justify a data retention period of five years.

A differentiator occurs however at the end of the data retention period. In the "normal" case, at the expiry of the data retention period of each entry/exit record calculated from the date of exit, the record is deleted. In case there are no more recent entry/exit records, the whole personal file is deleted, as the purpose of a personal file is to have entries and exits linked to it. In the case where overstay occurs, at the expiry of the date retention period there is still an entry record without an exit record. In that case, after five years calculated from the last possible day of authorised stay, the personal data and the entre/exit data are not deleted but removed from EES, handed over to each Member State for possible introduction into SIS. From that moment the data retention rules of SIS become applicable.

Data protection principles foresee that the retention of personal information shall be limited to the relevant purposes. A short data retention period is sufficient for achieving the second objective of the EES (i.e. to reduce irregular migration by addressing the phenomenon of overstaying) but would not be sufficient for facilitating the border crossing of bona fide travellers which is an essential element of the first objective. Therefore, in light of the above, a data retention period of five years, similar to the personal data anyhow stored in VIS, is considered sufficient and proportionate to the objective of facilitating the border crossing of bona fide travellers.

The 5 year length of the data retention period is also beneficial to the traveller. By having personal data, and in particular biometric data, stored over a relatively long period of time, the traveller is relieved from having to enrol his/her identity again at each entry to

the Schengen area. The enrolment step for visa-exempt travellers is indeed an additional step within the border control process introduced with the use of EES and, as such, requires time. Although benefits will accrue to the traveller at return visits, by lengthening the time-span between enrolments, that inconvenience can be mitigated. The same reasoning was applied for VIS where biometrics only need to be enrolled again after five years for similar reasons of convenience for the data subject.

Protection of data against risk of abuse?

The protection of data against risk of abuse refers in particular to the access to data and/or the transfer of data to persons to whom that access was not granted.

The main protection measures included in the regulation are:

– Access to EES is restricted to specific persons within designated Competent Authorities;

– Transfer of data to third parties, whether private or public entities is prohibited;

– All data processing is done by eu-LISA and therefore do not leave the EU.

A set of technical measures will further be developed and implemented as part of the security plan that must implemented during the development of EES.

13.3.7. Protection of other fundamental rights

The improved border control measures (aspects related to law enforcement are set out further) better implement:

– Article 5 ("The prohibition of slavery and force labour"). Victims of trafficking in human beings have been found among the category of overstayers and such situation can be suspected on the basis of the characteristics (age category, gender, country of origin to cite the obvious ones) recorded in EES. With EES these data are recorded for all countries and identify the date and place of entry which can lead to better detection at the border crossing point where this trafficking is occurring.

– Article 15.3 ("Nationals of third countries who are authorised to work in the territories of the Member States are entitled to working conditions equivalent to those of citizens of the Union."). This fundamental right becomes less relevant when there is an uncontrolled influx of irregular migrants who will accept any working conditions. The size and rate of increase of the number of overstayers is detrimental to the use of this right by third country nationals who use means of legal migration to stay and work in the EU.

The impact of EES on these fundamental rights further justifies the proportionality of the data collection.

13.3.8. Appropriate safeguards at EU level

A number of safeguards are integral to the proposed regulation, in particular for complying with fundamental rights:

– If there are errors on the identity checks of passengers, facilities are made available for carrying out manual checks and for amending the data on entry and exit at all

border crossing points. Regarding such facilities, the Schengen Borders Code currently requires that thorough second line checks for third-country nationals shall be carried out in a private area where the facilities exist and if requested by the third-country national.

– Individuals have the right to access information held on them and to challenge and correct it, if the processing of this data does not comply with the provisions of Directive 95/46 and Regulation 45/2001, in particular because of the incomplete or inaccurate nature of the data.

– Individuals are given the right to lodge a complaint with a data protection authority regarding the processing of their personal data and they are given the right to effective administrative and judicial remedies (Article 47 of the Charter).

– The guarantees ensuring an effective remedy (Article 47 of the Charter) for third-country nationals enable them to challenge a notification of an overstay by the entry/exit system, for example in situations when they were forced to overstay, particularly if it appears that they overstayed for a valid reason (e.g. hospitalisation, change in travel arrangements), when errors were made in recording dates of entry or exit or to show that they have a legal right to stay (e.g. based on a new visa, marriage to an EU citizen, application for asylum, refugee status).

– In case the EES notifies an overstay, this indication does not lead automatically to detention, removal or a sanction for the third-country national. Third-country nationals have access to effective remedies in such proceedings in order to protect the right to liberty and security (Art. 6 of the Charter), right to asylum (Art. 18 of the Charter), respect for family life (Art. 7 of the Charter) and the obligation of non-refoulement (Art. 19(2) of the Charter). A decision to detain, remove or sanction a third-country national is not based solely on a nofitication of overstay by the entry/exit system. In addition the safeguards of Directive 2008/115/EC are respected.

– The measures protecting rights of travellers, including right to an effective remedy, must also take into account the privileged position of non-EU family members of EU citizens whose right to enter and to stay depend on the right of the respective EU citizen in accordance with Directive 2004/38/EC.

13.3.9. Rights to Access and Correction

The rights to access and correction have already been developed under the section on "Appropriate safeguards", which deals not only with the right to access and correction but also with safeguards as regards the consequences for data subjects even when data are correct.

13.3.10. Control by an independent authority

Under the proposed regulation, the supervision of all data processing activities is carried out by Member States data protection authorities and the European Data Protection Supervisor which is conferred with all the necessary powers to intervene and enforce compliance with data protection rules.

13.3.11. Need for security and data protection by design and by default

The principles of data protection by design[11] and data protection by default are taken into account by implementing a set of very efficient data protection techniques already used in other large-scale IT systems (VIS in particular):

– The network used for the transmission of data from the central to the national domain uses encryption;

– The minimal data set is stored in EES (data minimisation principle[12]);

– Access to data is governed by access controls;

– All access to data is logged;

– All changes to data produce an audit trail.

The need for security translates into the implementation of a security plan that addresses physical and logical security of the data.

13.3.12. Conclusion

The authorities who should have access to the Entry Exit System must be designated for the specific purpose of the system. Therefore, access for consulting the data is reserved exclusively to duly authorised staff of the authorities of each Member State who are competent for the specific purposes of the Entry Exit System and limited to the extent the data are required for the performance of the tasks in accordance with these purposes.

All safeguards and mechanisms are in place for the effective protection of the fundamental rights of travellers particularly the protection of their private life and personal data. Third-country nationals must be made aware of these rights.

The EES hence respects the essence of the right to privacy, meets clearly defined objectives of general interest and is proportionate as the data stored in the EES strictly meet the legitimate objectives pursued by the Regulation and as the group of persons to whom it applies strictly corresponds to the ones affected by the applicable rule on duration of short stay.

Finally, it should be reminded that the EES helps to safeguard the fundamental rights of the European citizens provided under Article 5 of the Chart ("The prohibition of slavery and force labour") and Article 15.3 of the Chart ("Nationals of third countries who are authorised to work in the territories of the Member States are entitled to working conditions equivalent to those of citizens of the Union."). Furthermore, the use of modern IT systems, ABC gates and self-service kiosks at border controls can lead to a system less prone to discrimination as compared to checks performed by human beings and hence constitute an additional safeguard in terms of prohibition of discrimination (e.g. on the basis of race or ethnicity) in the meaning of Article 21 of the Chart.

---

[11] Privacy and Data protection by Design – from policy to engineering, Enisa (European Union Agency for Network and Information Security, December 2014.

[12] The withdrawal of the proposal of having the EES and the RTP as separate systems, in favour of a unique system also contributes to compliance with the data collection limitation and data minimisation principles.

13.4. Impact assessment for Law Enforcement Access

The approach followed states that in case access is given to Law Enforcement Services, the fundamental rights impact assessment needs to specifically re-do the test on necessity and proportionality:

Unlike in the 2013 proposal, in this proposed measure the objective "to contribute to the fight against terrorism and serious crime" appears as a secondary objective of the proposal. To meet this objective the access to EES data collected for immigration purposes are made accessible to Law Enforcement Authorities under precise conditions. It can be noted that Law Enforcement Authorities are given an access to immigration data and that no data are recorded in EES for another purpose than immigration control.

All the safeguards and control measures that apply to the EES data and explained under section 13.3 therefore remain valid and are not repeated under this section again.

The assessment therefore concentrates on the question of necessity and proportionality and on additional measures that protects the data subjects.

13.4.1. Necessity

This secondary objective is achieved by granting access to the EES database to Member States' law enforcement authorities and Europol in order to pursue the fight against terrorism and serious crimes under very specific and strict conditions. It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest. [13]

The Entry Exit system is the only system that collects the entry/exit data of all third-country nationals entering the Schengen area for a short stay, whether via a land, sea or air border. No other existing or envisaged data collection would even by far match the completeness of entry /exit data recorded in EES. As such for the purposes of criminal investigations, only EES can provide data to confirm or not the presence of specific third country nationals in the Schengen area. The EES also uses the identification data to link entries and exits and can act as the database of last resort for identifying persons when more focused databases did not yield a result.

The necessity of giving an access to EES data by law enforcement services has already been demonstrated by the situation with VIS. Although access bas been given only since two years to VIS data, there are more than 1.400 searches done on a monthly basis. Further thirteen countries have a national system in operations with entry-exit functionalities since many years. In all cases access to law enforcement authorities to the data recorded is granted and has demonstrated to fulfil a need.

The information contained in the Entry Exit system is necessary for the purposes of the prevention, detection and investigation of terrorist offences as referred to in Council Framework Decision 2002/475/JHA of 13 June 2002 on combatting terrorism or of other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

---

[13] See Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P *Al-Aqsa* v *Council* EU:C:2012:711, paragraph 130.

To meet the purposes mentioned in the previous paragraph there are two situations where the access to EES would be necessary:

– **Identification.** The data recorded in EES could support law enforcement authorities in the fight against terrorism and serious crime to establish the identity of a third country national both in cases where he/she destroyed his/her documents and when investigating a crime through the use of fingerprints or facial image. It should be noted that although the identification for law enforcement purposes is technically the same operation as the identification during inland control for immigration enforcement, the authority performing the check, the purpose (criminal responsibility vs verifying the right of stay) and the outcome of the control (potentially prosecution vs possible return decision) are very different in essence.

– **Criminal intelligence**. The data recorded in EES could also help to construct evidence by tracking the travel routes of a person suspected of having committed a crime or of a crime victim. Therefore, the data in the EES should be available, subject to the conditions set out in the regulation to the designated authorities of the Member States and the European Police Office (Europol).

"Cascade mechanism" for identification purposes. In case access to the EES is requested for identification of unknown suspects, perpetrators or victims of terrorist offences or other serious criminal offences, the principle is applied that more focused databases would be used before accessing the EES. In practice there is only the access to the data collected under the Prüm system that contains biometric data from known criminals that would meet this condition.

Data retention period. A data retention period of five years would be necessary also for the secondary purpose of the fight against terrorism and serious crime because in order to construct evidence in criminal cases by analysing data on travel routes, law enforcement authorities would have to be able to track the travel routes back for a period of several years. The data should be deleted after the period of five years, unless there are grounds to delete it earlier.

The data retention period has been determined on the basis of the experience gained with the use of the national systems recording entry/exit data at national level in thirteen Schengen Member States and which are all used, sometimes even primarily, by law enforcement authorities. The data retention periods range between five and twenty-five years and with one case where no deletion of data is envisaged at all. From Commission's evaluation and specific consultation of law enforcement authorities, the likelihood of having to access EES data beyond five years is not zero but follows a downward trend. The data retention period has therefore also been aligned to the ones for immigration purposes.

13.4.2. Proportionality

An essential element that meets the principle of proportionality is that access to data by law enforcement authorities would always be related to a specific case.

– Authorities could have access in well-defined cases, for identity verification and/or criminal intelligence purposes, when there is a substantiated suspicion that the perpetrator of a criminal offence could be registered in the EES. The proportionality principle requires that the EES be queried for such purposes only if there is an overriding public security concern, that is, if the act committed is so reprehensible that

it justifies querying a database that registers persons with a clean criminal record and the threshold for authorities responsible for internal security to query the EES must therefore always be significantly higher than the threshold for querying criminal databases.

– Access to the EES to request comparisons of data on the basis of a latent fingerprint, which is the dactyloscopic trace which may be found at a crime scene, is fundamental in the field of police cooperation. The possibility to compare a latent fingerprint with the fingerprint data which is stored in the EES in cases where there are reasonable grounds for believing that the perpetrator or victim may be registered in the EES will provide the authorities of the Member States with a very valuable tool in preventing, detecting or investigating terrorist offences or other serious criminal offences, when for example the only evidence at a crime scene are latent fingerprints.

13.4.3. Protection of other fundamental rights

Granting access to EES data by law enforcement authorities helps to safeguard the fundamental rights of the European citizen provided under the Chart:

– Article 2(1) ("Everyone has the right to life") Article 3(1) ("Everyone has the right to respect for his or her physical and mental integrity"), Article 5 ("Prohibition of slavery and force labour") and Article 6 ("Everyone has the right to liberty and security of persons"). The type of criminal offenses (terrorism and serious crime) for which law enforcement authorities would have access to EES, when all other conditions are met, are the ones that pose a serious threat to the lives of the citizens in the EU.

– Article 45(1) ("Every citizen of the Union has the right to move and reside freely within the territory of the Member States"). This applies in particular to terrorist offenses where the difficulty to prevent and counter-act leads authorities to re-install controls on all travellers within the EU reducing the use of the right contained in Article 45(1). The possibilities given to law enforcement authorities for a more effective fight against terrorism therefore also protects this fundamental right of EU citizens.

13.4.4. Specific Safeguards

Independent control of the reasons for access. A specific safeguard mechanism is provided in the regulation that ensures the independence and control of the Central Access Points and the operating units that initiate the requests for access. Requests for access to data stored in the Central System should be made by the operating units within the designated authorities to the Central Access Point and should be reasoned. The operating units within the designated authorities that are authorised to request access EES data should not act as a verifying authority. The Central Access Points should act independently of the designated authorities and should be responsible for ensuring, in an independent manner, strict compliance with the conditions for access as established in this regulation. The duly authorised staff of the Central Access Points should then process the request to the Central System following verification that all conditions for access are fulfilled. In exceptional cases of urgency, where early access is necessary to respond to a specific and actual threat related to terrorist offences or other serious criminal offences, the Central Access Point should process the request immediately and only carry out the verification afterwards.

Processing by Member State authorities. The processing of personal data by the authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences pursuant to this regulation should be subject to a standard of protection of personal data under their national law which complies with Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters .

Exchange of personal data. For the purpose of efficient comparison and exchange of personal data, Member States should fully implement and make use of the existing international agreements as well as of Union law concerning the exchange of personal data already in force, in particular of Decision 2008/615/JHA

Transfer of data to third parties. Transfers of personal data obtained by a Member State or Europol pursuant to this regulation for law enforcement purposes from the Central System to any third country or international organisation or private entity established in or outside the Union should be prohibited due to the potentially vast amount of data which could be shared and the risk of data mining. Certain third countries may also misuse access to data of their citizens for exercising repercussions on the members of their families still present in that third country.

13.4.5. Conclusion

Access to EES by law enforcement services fulfils a need that cannot be achieved by other measures, like access to another system. The data protection measures consist is granting this access only for specific categories of crimes (terrorism and serious crime), for specific purposes (criminal intelligence and criminal identification) related to specific cases, to specific authorities, using a specific control mechanism and in the case of criminal identification when the search was first conducted vs criminal databases before accessing the EES data. And on top of this, the independent control and safeguard mechanisms applicable to EES data continue to prevail.

Finally it should be reminded that granting access to EES data by law enforcement helps to safeguard the fundamental rights of the European citizens provided under Article 2(1) of the Chart ("Everyone has the right to life"), Article 3(1) of the Chart ("Everyone has the right to respect for his or her physical and mental integrity"), Article 5 of the Chart ("Prohibition of slavery and force labour")Article 6 of the Chart ("Everyone has the right to liberty and security of persons") and Article 45(1) of the Chart ("Every citizen of the Union has the right to move and reside freely within the territory of the Member States").

14. ANNEX 14: EXECUTIVE SUMMARY OF RESULTS FROM 2015 PILOT[14]

Adobe Acrobat Document

[14] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_executive_summary_en.pdf

15. ANNEX 15: FUNDAMENTAL RIGHTS AGENCY SURVEY - REPORT[15]

Adobe Acrobat Document

[15] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf (see section 7)

16. ANNEX 16: PREPARATORY WORK WITH THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

On 12 December 2014, DG HOME consulted the EDPS in the context of the preparation of the Smart Borders Pilot. A meeting was organised to discuss the provisions concerning personal data protection to be foreseen in the delegation agreement entrusting the implementation of the Smart Borders pilot to eu-LISA. The outcomes of this meeting were inserted in the delegation agreement.

On 20 March 2015, DG HOME and EDPS jointly organised a workshop on the preparation of the Smart Borders proposals. The outcome of this workshop is summarised below.

On 21 September 2015, some questions related to the Smart Borders were discussed in an interactive workshop between DG HOME and EDPS focussing on "Data Protection and Privacy Considerations in Policies on Migration and Home Affairs".

* * *

Proceedings of the 20 March 2015 workshop on Smart Borders proposals.

1. Introduction by the EDPS

The EDPS gave a presentation on the impact of the judgment of the Court of 8 April 2014 in Joined Cases C-293/12 and C-594-12 Digital Rights Ireland and Seitlinger and Others for the Smart Borders proposals. The EDPS also pointed out that the EP Legal Services' Opinion sets out a method for reviewing the validity of acts under Articles 7, 8 and 52 of the Charter, which include a number of factors to be considered. The main issue will be the possible addition of a secondary purpose to the EES proposal, namely the use of entry and exit data and biometrics for law enforcement purposes. The necessity and proportionality test will have to be taken and passed separately for the two possible purposes of the EES proposal. DG HOME said its analysis of the data retention ruling was the same as that of the EDPS and said it looked forward to working with the EDPS on building the blocks of LEA for this and other files.

The EDPS touched upon Privacy by Design and emphasized as a first step the need for a specific legislative text to embed concrete appropriate safeguards as regards data protection and security. Those safeguards should lead to ensuring that the design of the IT system respects data protection principles. The specific technical and security measures required in developing and protecting the IT system need not be embedded in the legislative text itself, but preferably should be developed later in separate documents when the legislative text is near finalisation. With regard to the envisaged website for information to carriers and travellers, the EDPS said that there was a business need to do this and that the legal base should contain a high enough level of details on it.

2. Biometrics in the Smart Borders package

DG HOME gave a presentation on the use of biometrics in the Smart Borders package and the need thereof to improve border control processes, especially for third country

nationals from visa-free countries. DG HOME informed the EDPS that probably there will be no duplication of data for visa holders of whom 10 fingerprints should already be in the Visa Information System. Also the combined use of fewer fingerprints with facial images will be tested during the Pilot Project.

DG HOME and the EDPS had a preliminary discussion on data protection considerations and clarified important elements of their respective analysis. The importance of distinguishing the use of data for verification/control purposes from identification purposes was underlined in relation to the processing of biometrics data, in the sense that identification requires more biometric data (such as fingerprints and a facial image) and cannot rely on facial image only.

3. Data retention

DG HOME gave a presentation on the data retention rules in the 2013 proposals, the drawbacks of those rules, the mains findings of the Technical Study and the different options proposed by the Study.

DG HOME and the EDPS discussed the possible extension of the initial data retention period for the objective of improving the management of the external borders in order to avoid frequent registration of travellers in the system. They also discussed the need for extending the data retention period for the secondary purpose of law enforcement access. The EDPS underlined that the first question to be answered is the length for which it is necessary to retain data in the EES in view of the original purpose pursued. Then as concerns law enforcement access, there should be a thorough evaluation of the necessity of law enforcement access to the data. Even if in theory one could imagine that the initial retention period could be increased for an additional time on the basis of law enforcement access demonstrated needs, the EDPS mentioned that such an extension could only be valid if it respects the conditions of necessity and proportionality and provided that appropriate safeguards are implemented.

4. Necessity of access to EES for law enforcement purposes

The EDPS gave a presentation of their Policy Paper "Analysing the impact of privacy and data protection of EU legislative proposals", which outlines the different steps taken by the EDPS when consulted on a legislative proposal.

DG HOME gave a presentation on the necessity of access to the EES for law enforcement purposes and the foreseen requirements. DG HOME reported on the conclusions of the EES Impact Assessment and the findings of the Study. From those documents, it appears that a 5-years retention period would be appropriate should law enforcement access be granted. DG HOME also reported on the state of play of discussions in the Council on LEA to the EES proposal and noted that most delegations want to have access to all data stored in the EES for a period of 5 years. DG HOME referred to the explanations of MS on the added value of LEA to the national entry/exit systems and the VIS and the specific examples they had given of the added value of LEA in solving cases concerning murder, smuggling of irregular immigrants, procurement for prostitution and narcotics, stolen vehicles, human and drug trafficking, state security and terrorism. DG HOME and the EDPS exchanged their views on the possible extension of the data retention period to 5 years for law enforcement purposes, taking into account differentiated access. The EDPS noted that differentiated access could make sense and insisted on the need for adequate safeguards but did not express any views on the question by DG HOME on the possible use of the VIS or the Eurodac model for the

proposal and on possible improvements which could be considered the reason being that the access procedure will need to follow the needs determined as necessary (i.e. this cannot be answered in the abstract). The EDPS mentioned its Opinion of 2011 on the Evaluation report from the Commission on the Data Retention Directive, which contains useful indications as to what kind of evidence is expected in order to demonstrate the necessity of an interfering measure.

The representative of the LS underlined the need to understand the precise uses that the law enforcement authorities would want to make of the system and the type of researches that they could need to carry out in different types of investigation. He suggested as hypothetical examples that LEA in the context of criminal investigations regarding crimes closely linked to illegal immigration (such as trafficking in human beings) might be considered differently from LEA to the same database in the context of investigating other crimes (such as murder): in the first case one of the constituent elements of the crime is bringing third country nationals illegally into the Union, which includes the crossing of the external border which is registered in the EES, whereas in the second case one would presumably check the EES for the remote possibility that the fingerprints found next to the deceased body are present in the database. The LS underlined the urgency to get down to detailed conversations with law enforcement specialists to hear in which precise investigation contexts they considered LEA to the EES of very high utility.

5. Requirements for communication of data to third countries

DG HOME gave a presentation on the requirements for communication of data to third countries included in Article 27 of the current EES proposal and explained that Article 46 of the proposal provides that the question of whether access to EES data to LE authorities of third countries shall be granted should be part of the evaluation to be conducted two years after the EES entered into operation.

DG HOME asked the EDPS on the way the conditions foreseen in Article 27 of the 2013 EES Proposal could be further substantiated as it had suggested in its opinion on the EES proposal. As regards the possible granting of access to law enforcement authorities of third countries, the EDPS referred again to the guarantees under the DRD ruling. DG HOME also asked the EDPS whether there should be a prohibition of transfers to third-country LEAs as is the case in the Eurodac Regulation or whether such access should be allowed in exceptional cases as in the VIS decision. The EDPS replied that the implementation of the different legal instruments should be examined carefully and noted it was premature to make an evaluation in this regard.

6. RTP: Use of MRTD instead of the token : data protection issues

7. RTP on-line application process.

8. Option to improve RTP efficiency

The points 7, 8 and 9 of the agenda were discussed altogether.

DG HOME presented the different options analysed by the Study for the RTP and their pros and cons; i.e. the use of a separate token, of an e-MRTD or of a MRTD. DG HOME and the EDPS exchanged their views on the use of the e-MRTD as the token for the RTP. The EDPS would need to look at the details of the different options in order to make informed comments on the options.

With regard to the RTP on-line application process, DG HOME and the EDPS discussed the possibility of redirecting the data submitted by the applicants to the competent Member State. The different architectures for the Webservice were also touched upon during the discussion.

17. ANNEX 17: EXISTING EU LARGE-SCALE IT SYSTEMS

17.1. Overview

This annex gives an overview of currently existing European large-scale IT systems. There are three European Large Scale IT systems:

– SIS: the centralised database containing alerts on persons and other categories of data for law enforcement and border check purposes (SIS);

– VIS: the database on visa applications. VIS uses a Biometric Matching System (BMS) which is established as a service that could be used by other systems (like EES in the future);

– Eurodac: the database on asylum applicants.

The EU Agency for large-scale IT systems, euLISA, is responsible for the operational management of these three systems including the BMS.

A police co-operation mechanism for exchanging information on DNA, fingerprints and vehicle registration data has been established through the Prüm Decisions. However the exchanges are happening between Member States and there is no central system.

Advanced Passenger Information (API) and Personal Name Records (PNR) are data sent by carriers to national authorities but there is no European system where these data are stored.

17.2. Legal instruments

The legal instruments for the three existing large-scale IT system are presented in the table below.

	Instrument	Description
SIS (II)	Regulation (EC) No 1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)	This Regulation establishes the conditions and procedures for the entry and processing in SIS II of alerts in respect of third-country nationals, the exchange of supplementary information and additional data for the purpose of refusing entry into, or stay in, a Member State. The Regulation also lays down provisions on the technical architecture of SIS II, the responsibilities of the Member States and of the management authority referred in to Article 15, general data processing, the rights of the persons concerned and liability.
	Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)	The Decision establishes the conditions and procedures for the entry and processing in SIS II of alerts on persons and objects, the exchange of supplementary information and additional data for the purpose of police and judicial cooperation in criminal matters. The Decision also lays down provisions on the technical architecture of SIS II, the responsibilities of the Member States and of the

		engagement authority referred to in Article 15, general data processing, the rights of the persons concerned and liability.
VIS	Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)	The Regulation defines the purpose of, the functionalities of and the responsibilities for the Visa Information System as established by Article 1 of Decision 2004/512/EC. The Regulation sets up the conditions and procedures for the exchange of data between Member States on applications for short-stay visas and on the decisions taken in relation thereto, including the decision whether to annul, revoke or extend the visa, to facilitate the examination of such applications and the related decisions.
	Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences	This Decision lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may obtain access for consultation of the Visa Information System for the purposes of prevention, detection and investigation of terrorist offences and of other serious criminal offences.
Eurodac	Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention	The Regulation establishes the Eurodac system which aims to assist in determining which Member State is to be responsible pursuant to the Dublin Convention for examining an application for asylum lodged in a Member State, and otherwise to facilitate the application of the Dublin Regulation under the conditions set out in the Regulation. This Regulation has been repealed with effect from 20 July 2015 by Regulation (EU) No 603/2013 (Eurodac recast Regulation) quoted further down.
	Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000	This Regulation establishes rules for the transmission of data , for carrying out comparisons and transmitting results, for the communication between Member States and the Central Unit and for other tasks of the Central unit. This Regulation has been repealed with effect from 20 July 2015 by Regulation (EU) No 603/2013 (Eurodac recast Regulation) quoted further down.
	Regulation (EU) No 603/2013 of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of	Eurodac amendment amending Regulation (EU) No 1077/2011 Eu-LISA was entrusted with the Commission's tasks relating to the operational management of Eurodac and with certain tasks relating to the Communication Infrastructure in accordance with

	Regulation (EU) No 604/2013 and amending Regulation (EU) No 1077/2013	Article 5 of the Agency establishing Regulation. This provision has been amended by Article 38(1) of the Eurodac recast Regulation

17.3. Schengen Information System

The Schengen Information System (SIS) is a large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The SIS enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. A SIS alert not only contains information about a particular person or object but also clear instructions on what to do when the person or object has been found. Specialised national SIRENE Bureaux serve as single points of contact for any supplementary information exchange and coordination of activities related to SIS alerts.

Purpose of SIS

The main purpose of the SIS is to help preserving internal security in the Schengen States in the absence of internal border checks.

Which countries use SIS?

The SIS is in operation in all EU Member States and Associated Countries that are part of the Schengen Area. Special conditions exist for EU Member States that are not part of the Schengen Area.

– EU Member States that are part of the Schengen Area. The Schengen Area encompasses most EU Member States, except for Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom. The 22 EU Member States that are part of the Schengen Area fully operate the SIS.

– Associated Countries that are part of the Schengen Area. Four Associated Countries that are part of the Schengen Area (Switzerland, Norway, Liechtenstein and Iceland) fully operate the SIS.

– Bulgaria, Croatia, Cyprus, Ireland, Romania and United Kingdom. Bulgaria and Romania currently only operate the SIS only for the purpose of law enforcement cooperation. They will start using the SIS for the purpose of external border control as soon as the decision for lifting the internal border checks has entered into effect. Cyprus and Croatia are enjoying a temporary derogation from joining the Schengen Area. They are currently carrying out preparatory activities to integrate into the SIS. The United Kingdom operates the SIS within the context of law enforcement cooperation. Ireland is carrying out preparatory activities to integrate into the SIS for the purpose of law enforcement cooperation.

How does it work?

The SIS operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system. The SIS enables the users to check persons and objects both at external borders and within the territory of the Schengen States. The SIS provides law enforcement authorities

with information on why a certain individual is wanted, what action is to be taken and whether the person is presumed violent and armed.

However, as the information contained in the SIS is only sufficient for the authorities on the ground to take the correct initial actions it is necessary for the Member States to be able to exchange supplementary information, either on a bilateral or multilateral basis, as required for implementing certain provisions of the Schengen Convention, and to ensure full application of Title IV of the Schengen Convention for the SIS as a whole.

Article 92(4) of the Schengen Convention provides that Member States shall, in accordance with national legislation, exchange through the authorities designated for that purpose (SIRENE), all information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons in respect of whom, and objects in respect of which, data have been entered in the Schengen Information System, are found as a result of searches made in this System.

The Schengen States are the owners of the data they introduce into the SIS and bear the responsibility for their legality and accuracy.

What does the SIS contain?

The SIS only contains alerts on persons or objects falling under one of the following alert categories:

– Refusal of entry or stay (Article 24 of Regulation (EC) No 1987/2006) This alert category covers third-country nationals who are not entitled to enter into or stay in the Schengen Area.

– Persons wanted for arrest (Article 26 of Council Decision 2007/533/JHA) This alert category covers persons for whom a European Arrest Warrant or Extradition Request (Associated Countries) has been issued.

– Missing persons (Article 32 of Council Decision 2007/533/JHA) The purpose of this alert category is to find missing persons, including children, and to place them under protection if lawful and necessary.

– Persons sought to assist with a judicial procedure (Article 34 of Council Decision 2007/533/JHA) The purpose of this alert category is to find out the place of residence or domicile of persons sought to assist with criminal judicial procedures (for example witnesses).

– Persons and objects for discreet or specific checks (Article 36 of Council Decision 2007/533/JHA) The purpose of this alert is to obtain information on persons or related objects for the purposes of prosecuting criminal offences and for the prevention of threats to public or national security.

– Objects for seizure or use as evidence in criminal procedures (Article 38 of Council Decision 2007/533/JHA) This alert covers objects (for example vehicles, travel documents, credit cards, number plates and industrial equipment) being sought for the purposes of seizure or use as evidence in criminal proceedings.

Who can access SIS?

The Schengen Information System (SIS) provides access to alerts on persons and objects to the following authorities:

– authorities responsible for border checks;

– authorities carrying out and coordinating other police and customs checks within the country;

– national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation;

– authorities responsible for issuing visas, the central authorities responsible for examining visa applications, authorities responsible for issuing residence permits and for the administration of legislation on third-country nationals in the context of the application of the Union acquis relating to the movement of persons;

– authorities responsible for issuing vehicle registration certificates.

It is up to each Member State to decide which national authorities are competent and shall have access to some or all categories of SIS alerts depending on that competence.

Europol and Eurojust also have access to certain categories of alerts. Europol may access data entered for alerts for arrest, alerts for discreet surveillance or specific check and alerts on objects for seizure or use as evidence in criminal proceedings. Eurojust may access data entered for alerts for arrest and alerts for a judicial procedure.

Which data on persons are stored?

In 2015, about one million records exist on wanted persons. The vast majority of alerts on persons are about third-country nationals who shall be denied entry to the Schengen area.

As regards these individuals, the SIS currently stores only alphanumeric data (letters and numbers):

– names, including aliases;

– sex;

– objective physical characteristics "not subject to change";

– date and place of birth;

– nationality;

– whether the persons are armed or violent;

– the reason for the alert; and

– the action to be taken.

The alerts on persons may contain a picture or biometric information but only as attachments to the file and this information is not searchable. This means that a person cannot be found back in SIS on the basis of his/her fingerprints or picture. But once a person is found the picture and/or fingerprints can be used to ascertain the identity.

17.4. Visa Information System

The Visa Information System (VIS) is a system for the exchange of short-stay visa data between the Schengen and the Schengen Associated States that was initially established in 2004.

The Visa Information System (VIS) allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

All functionalities of the VIS are based on visa applications or visa decisions attached to applications. After a first registration, a visa application can be amended, until a decision is made whether or not a Schengen visa should be issued. After visa issuance, further decisions can be made, for example, an issued visa can be revoked or annulled, or a visa can be extended. The VIS supports the storage, maintenance and retrieval of this information.

Purposes of the VIS

– Facilitating checks and the issuance of visas: VIS enables border guards to verify that a person presenting a visa is its rightful holder and to identify persons found on the Schengen territory with no or fraudulent documents. Using biometric data to confirm a visa holder's identity allows for faster, more accurate and more secure checks. The system also facilitates the visa issuance process, particularly for frequent travellers.

– Fighting abuses: While the very large majority of visa holders follow the rules, abuses can also take place. For instance, VIS will help in fighting and preventing fraudulent behaviours, such as "visa shopping" (i.e. the practice of making further visa applications to other EU States when a first application has been rejected).

– Protecting travellers: Biometric technology enables the detection of travellers using another person's travel documents and protects travellers from identity theft.

– Helping with asylum applications: VIS makes it easier to determine which EU State is responsible for examining an asylum application and to examine such applications.

– Enhancing security: VIS assists in preventing, detecting and investigating terrorist offences and other serious criminal offences.

How does it work in practice?

Ten fingerprints and a digital photograph are collected from persons applying for a visa. These biometric data, along with data provided in the visa application form, are recorded in a secure central database.

Ten finger scans are not required from children under the age of 12 or from people who physically cannot provide finger scans. Frequent travellers to the Schengen Area do not have to give new finger scans every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a 5-year period.

At the Schengen Area's external borders, the visa holder's finger scans may be compared against those held in the database. A mismatch does not mean that entry will automatically be refused - it will merely lead to further checks on the traveller's identity.

Who can access VIS?

Competent visa authorities may consult the VIS for the purpose of examining applications and decisions related thereto.

The authorities responsible for carrying out checks at external borders and within the national territories have access to search the VIS for the purpose of verifying the identity of the person, the authenticity of the visa or whether the person meets the requirements for entering, staying in or residing within the national territories.

Asylum authorities only have access to search the VIS for the purpose of determining the EU State responsible for the examination of an asylum application.

According to Council Decision 2008/633/JHA of 23 June 2008, law enforcement authorities from Member States and Europol have a restricted and indirect access to the VIS data for the purposes of preventing, detecting and investigating terrorist and criminal offences. Each Member State has to designate an authority responsible for controlling law enforcement access to the database and the police have to provide evidence that their query is necessary for criminal investigations.

Which data are stored?

According to the text of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008, the VIS stores the following personal data from visa applicants:

– Data on the applicant (i.e. name, address, occupation);

– Data on the visa application process (date and place of the application, visas requested, issued, refused, annulled, revoked or extended);

– Biometrics (photographs and fingerprints).

Current Status

The VIS started operations in the first region on 11 October 2011. The operations started first at the consulates in North Africa and 20 days after go-live of the VIS also at the border crossing points (verification of visas against the VIS).

Biometric verification of the visas is mandatory at entry into the Schengen area since 11 October 2013.

Since 20 November 2015, the "roll-out" was completed, meaning that all visas issued by consulates from Schengen Member States are recorded in VIS and contain biometrics.

17.5. Biometric Matching System

The Biometric Matching System (BMS) developed for the VIS is an information search engine that can match biometric data from visa applications, identity management systems and policing systems.

The system performs one-to-one comparisons for biometric verifications and one-to-many searches for biometric identifications.

The BMS is developed using a service-oriented architecture approach, has the capability to connect with a number of IT systems and manage functions related to visas, immigration, border control and police cooperation. In addition, the technical architecture is flexible enough to accommodate new developments in EU policy as immigration and border control procedures evolve.

BMS does not store biometric information as such which is owned by the requesting system. As an example, since currently BMS only operates with VIS, fingerprints and photo are stored in VIS. For each fingerprint, the template[16] is stored in BMS. BMS provides the service of matching fingerprints on the request of the systems that it is linked to, currently only VIS but this can be extended when authorised. The current BMS does not use the facial image as a biometric identifier. This means that while pictures are stored in VIS there is no template equivalent created in BMS. Hence with the current VIS and BMS, the facial image cannot be used to search for a person or match a picture taken live with a picture stored in VIS. However the existing BMS can be enhanced with this functionality and does not require to be replaced.

17.6. Eurodac

The Eurodac Regulation establishes an EU asylum fingerprint database. The previous version of the Regulation was still valid until 20 July 2015 when the new one became applicable. When someone applies for asylum, no matter where they are in the EU, their fingerprints are transmitted to the Eurodac central system.

Updates to the relevant legislation establishing Eurodac were required to reduce the delay of data transmission by the Member States, to precipitate the asylum procedure, to address data protection concerns as well as to help combatting terrorism and serious crime by allowing law enforcement access to Eurodac. The new requirements were laid down in the Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 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 ('recast regulation').

The Eurodac system enables Member States to identify asylum applicants and persons who have been apprehended while unlawfully crossing an external frontier of the Community. By comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State or whether an asylum applicant entered the Union territory unlawfully.

[16] A template is a stored record of an individual's biometric features. Typically, a "livescan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template

The Eurodac central unit operates a central database comparing fingerprints, an automated fingerprint identification system (AFIS) and a secure communication system for data transmission from and towards the national units (National Access Points) in Member States.

Data collected for any asylum applicants over 14 years of age include:

– Fingerprint and control images;

– Date of the asylum application;

– The Member State where the asylum application was filed;

– The gender of the applicant.