



EUROPEAN COMMISSION
Research Executive Agency (REA)

Director



GRANT AGREEMENT

NUMBER — 700626 — iCROSS

This **Agreement** ('the Agreement') is **between** the following parties:

on the one part,

*the **Research Executive Agency (REA)** ('the Agency'), under the power delegated by the European Commission ('the Commission')¹,*

represented for the purposes of signature of this Agreement by [REDACTED], Research Executive Agency (REA), Industrial Leadership and Societal Challenges Department, Safeguarding Secure Society, [REDACTED],

and

on the other part,

1. 'the coordinator':

EUROPEAN DYNAMICS LUXEMBOURG SA (ED) SA, [REDACTED] established in RUE JEAN ENGLING 12, LUXEMBOURG 1466, Luxembourg, [REDACTED] represented for the purposes of signing the Agreement by [REDACTED]

and the following other beneficiaries, if they sign their 'Accession Form' (see Annex 3 and Article 56):

2. **INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS),** [REDACTED], established in Patission Str. 42, ATHINA 10682, Greece, [REDACTED]

3. **STREMBLE VENTURES LTD (STR) CY1,** [REDACTED], established in KO 8 GERMASOGEIA, LIMASSOL 4045, Cyprus, [REDACTED],

4. **THE MANCHESTER METROPOLITAN UNIVERSITY (MMU),** N/A, established in All Saints Building Oxford Road, MANCHESTER M15 6BH, United Kingdom, [REDACTED]

5. **ITTI SP ZOO (ITTI) SP(ZOO),** [REDACTED], established in RUBIEZ 46, POZNAN 61 612, Poland, [REDACTED]

6. **EVERIS AEROSPACIAL Y DEFENSA SL (EVR) SL,** [REDACTED] established in AVENIDA DE MANOTERAS 52, MADRID 28050, Spain, [REDACTED]

7. **BIOSEC GROUP KORLATOLT FELELOSSEGU TARSASAG (BIO) KFT,** [REDACTED], established in ANDY ENDRE UTCA 19, BUDAPEST 1024, Hungary, [REDACTED],

8. **JAS TECHNOLOGIE SP ZOO (JAS) SP(ZOO),** [REDACTED] established in UL. WISNIOWA 40 LOK 6, WARSZAWA 02 520, Poland, [REDACTED],

9. **GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER (LUH),** established in Welfengarten 1, HANNOVER 30167, Germany, [REDACTED]

¹ Text in *italics* shows the options of the Model Grant Agreement that are applicable to this Agreement.

10. **ORSZAGOS RENDOR - FOKAPITANYSAG (HNP)**, established in TEVE U. 4-6, BUDAPEST 1139, Hungary,

11. **KOMENDA GLOWNA STRAZY GRANICZNEJ (PBG)**, established in AL. NIEPODLEGLOSCI 100, WARSZAWA 02514, Poland,

12. **TRAINOSE METAFORES-METAFORIKES YPIRESIES EPIVATON KAI FORTIOU AE (TRA)**, established in KAROLOU STR 1 3, ATHINA 10437 , Greece,

13. **LATVIAN STATE BORDER GUARD (BSG)**, established in RUDOLFA STREET 5, RIGA LV-1012, Latvia,

Unless otherwise specified, references to ‘beneficiary’ or ‘beneficiaries’ include the coordinator.

The parties referred to above have agreed to enter into the Agreement under the terms and conditions below.

By signing the Agreement or the Accession Form, the beneficiaries accept the grant and agree to implement it under their own responsibility and in accordance with the Agreement, with all the obligations and conditions it sets out.

The Agreement is composed of:

Terms and Conditions

Annex 1	Description of the action
Annex 2	Estimated budget for the action
Annex 3	Accession Forms
Annex 4	Model for the financial statements
Annex 5	Model for the certificate on the financial statements
Annex 6	Model for the certificate on the methodology

TERMS AND CONDITIONS

TABLE OF CONTENTS

CHAPTER 1 GENERAL.....	11
ARTICLE 1 — SUBJECT OF THE AGREEMENT.....	11
CHAPTER 2 ACTION.....	11
ARTICLE 2 — ACTION TO BE IMPLEMENTED.....	11
ARTICLE 3 — DURATION AND STARTING DATE OF THE ACTION.....	11
ARTICLE 4 — ESTIMATED BUDGET AND BUDGET TRANSFERS.....	11
4.1 Estimated budget.....	11
4.2 Budget transfers.....	11
CHAPTER 3 GRANT.....	11
ARTICLE 5 — GRANT AMOUNT, FORM OF GRANT, REIMBURSEMENT RATES AND FORMS OF COSTS.....	11
5.1 Maximum grant amount.....	11
5.2 Form of grant, reimbursement rates and forms of costs.....	12
5.3 Final grant amount — Calculation.....	12
5.4 Revised final grant amount — Calculation.....	14
ARTICLE 6 — ELIGIBLE AND INELIGIBLE COSTS.....	14
6.1 General conditions for costs to be eligible.....	14
6.2 Specific conditions for direct costs to be eligible.....	15
6.3 Conditions for costs of linked third parties to be eligible.....	21
6.4 Conditions for in-kind contributions provided by third parties free of charge to be eligible.....	21
6.5 Ineligible costs.....	21
6.6 Consequences of declaration of ineligible costs.....	21
CHAPTER 4 RIGHTS AND OBLIGATIONS OF THE PARTIES.....	22
SECTION 1 RIGHTS AND OBLIGATIONS RELATED TO IMPLEMENTING THE ACTION.....	22
ARTICLE 7 — GENERAL OBLIGATION TO PROPERLY IMPLEMENT THE ACTION.....	22
7.1 General obligation to properly implement the action.....	22
7.2 Consequences of non-compliance.....	22
ARTICLE 8 — RESOURCES TO IMPLEMENT THE ACTION — THIRD PARTIES INVOLVED IN THE ACTION.....	22

ARTICLE 9 — IMPLEMENTATION OF ACTION TASKS BY BENEFICIARIES NOT RECEIVING EU FUNDING.....	22
ARTICLE 10 — PURCHASE OF GOODS, WORKS OR SERVICES.....	22
10.1 Rules for purchasing goods, works or services.....	22
10.2 Consequences of non-compliance.....	23
ARTICLE 11 — USE OF IN-KIND CONTRIBUTIONS PROVIDED BY THIRD PARTIES AGAINST PAYMENT.....	23
11.1 Rules for the use of in-kind contributions against payment.....	23
11.2 Consequences of non-compliance.....	24
ARTICLE 12 — USE OF IN-KIND CONTRIBUTIONS PROVIDED BY THIRD PARTIES FREE OF CHARGE.....	24
12.1 Rules for the use of in-kind contributions free of charge.....	24
12.2 Consequences of non-compliance.....	24
ARTICLE 13 — IMPLEMENTATION OF ACTION TASKS BY SUBCONTRACTORS.....	24
13.1 Rules for subcontracting action tasks.....	24
13.2 Consequences of non-compliance.....	25
ARTICLE 14 — IMPLEMENTATION OF ACTION TASKS BY LINKED THIRD PARTIES.....	25
ARTICLE 15 — FINANCIAL SUPPORT TO THIRD PARTIES.....	25
15.1 Rules for providing financial support to third parties.....	25
15.2 Financial support in the form of prizes.....	25
15.3 Consequences of non-compliance.....	25
ARTICLE 16 — PROVISION OF TRANS-NATIONAL OR VIRTUAL ACCESS TO RESEARCH INFRASTRUCTURE.....	26
16.1 Rules for providing trans-national access to research infrastructure.....	26
16.2 Rules for providing virtual access to research infrastructure.....	26
16.3 Consequences of non-compliance.....	26
SECTION 2 RIGHTS AND OBLIGATIONS RELATED TO THE GRANT ADMINISTRATION.....	26
ARTICLE 17 – GENERAL OBLIGATION TO INFORM.....	26
17.1 General obligation to provide information upon request.....	26
17.2 Obligation to keep information up to date and to inform about events and circumstances likely to affect the Agreement.....	26
17.3 Consequences of non-compliance.....	27
ARTICLE 18 — KEEPING RECORDS — SUPPORTING DOCUMENTATION.....	27
18.1 Obligation to keep records and other supporting documentation.....	27
18.2 Consequences of non-compliance.....	28
ARTICLE 19 — SUBMISSION OF DELIVERABLES.....	28
19.1 Obligation to submit deliverables.....	28

19.2 Consequences of non-compliance.....	28
ARTICLE 20 — REPORTING — PAYMENT REQUESTS.....	28
20.1 Obligation to submit reports.....	28
20.2 Reporting periods.....	29
20.3 Periodic reports — Requests for interim payments.....	29
20.4 Final report — Request for payment of the balance.....	30
20.5 Information on cumulative expenditure incurred.....	31
20.6 Currency for financial statements and conversion into euro.....	31
20.7 Language of reports.....	31
20.8 Consequences of non-compliance — Suspension of the payment deadline — Termination.....	31
ARTICLE 21 — PAYMENTS AND PAYMENT ARRANGEMENTS.....	31
21.1 Payments to be made.....	31
21.2 Pre-financing payment — Amount — Amount retained for the Guarantee Fund.....	31
21.3 Interim payments — Amount — Calculation.....	32
21.4 Payment of the balance — Amount — Calculation — Release of the amount retained for the Guarantee Fund.....	32
21.5 Notification of amounts due.....	33
21.6 Currency for payments.....	33
21.7 Payments to the coordinator — Distribution to the beneficiaries.....	34
21.8 Bank account for payments.....	34
21.9 Costs of payment transfers.....	34
21.10 Date of payment.....	34
21.11 Consequences of non-compliance.....	34
ARTICLE 22 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS.....	35
22.1 Checks, reviews and audits by the <i>Agency and the Commission</i>	35
22.2 Investigations by the European Anti-Fraud Office (OLAF).....	37
22.3 Checks and audits by the European Court of Auditors (ECA).....	37
22.4 Checks, reviews, audits and investigations for international organisations.....	37
22.5 Consequences of findings in checks, reviews, audits and investigations —Extension of findings.....	37
22.6 Consequences of non-compliance.....	39
ARTICLE 23 — EVALUATION OF THE IMPACT OF THE ACTION.....	39
23.1 Right to evaluate the impact of the action.....	39
23.2 Consequences of non-compliance.....	40
SECTION 3 RIGHTS AND OBLIGATIONS RELATED TO BACKGROUND AND RESULTS.....	40

SUBSECTION 1 GENERAL.....	40
ARTICLE 23a — MANAGEMENT OF INTELLECTUAL PROPERTY.....	40
23a.1 Obligation to take measures to implement the Commission Recommendation on the management of intellectual property in knowledge transfer activities.....	40
23a.2 Consequences of non-compliance.....	40
SUBSECTION 2 RIGHTS AND OBLIGATIONS RELATED TO BACKGROUND.....	40
ARTICLE 24 — AGREEMENT ON BACKGROUND.....	40
24.1 Agreement on background.....	40
24.2 Consequences of non-compliance.....	41
ARTICLE 25 — ACCESS RIGHTS TO BACKGROUND.....	41
25.1 Exercise of access rights — Waiving of access rights — No sub-licensing.....	41
25.2 Access rights for other beneficiaries, for implementing their own tasks under the action.....	41
25.3 Access rights for other beneficiaries, for exploiting their own results.....	41
25.4 Access rights for affiliated entities.....	42
25.5 Access rights for third parties.....	42
25.6 Consequences of non-compliance.....	42
SUBSECTION 3 RIGHTS AND OBLIGATIONS RELATED TO RESULTS.....	42
ARTICLE 26 — OWNERSHIP OF RESULTS.....	42
26.1 Ownership by the beneficiary that generates the results.....	42
26.2 Joint ownership by several beneficiaries.....	43
26.3 Rights of third parties (including personnel).....	43
26.4 <i>Agency</i> ownership, to protect results.....	43
26.5 Consequences of non-compliance.....	44
ARTICLE 27 — PROTECTION OF RESULTS — VISIBILITY OF EU FUNDING.....	44
27.1 Obligation to protect the results.....	44
27.2 <i>Agency</i> ownership, to protect the results.....	45
27.3 Information on EU funding.....	45
27.4 Consequences of non-compliance.....	45
ARTICLE 28 — EXPLOITATION OF RESULTS.....	45
28.1 Obligation to exploit the results.....	45
28.2 Results that could contribute to European or international standards — Information on EU funding.....	45
28.3 Consequences of non-compliance.....	46
ARTICLE 29 — DISSEMINATION OF RESULTS — OPEN ACCESS — VISIBILITY OF EU FUNDING.....	46
29.1 Obligation to disseminate results.....	46

29.2 Open access to scientific publications.....	46
29.3 Open access to research data.....	47
29.4 Information on EU funding — Obligation and right to use the EU emblem.....	47
29.5 Disclaimer excluding <i>Agency</i> responsibility.....	47
29.6 Consequences of non-compliance.....	47
ARTICLE 30 — TRANSFER AND LICENSING OF RESULTS.....	48
30.1 Transfer of ownership.....	48
30.2 Granting licenses.....	48
30.3 <i>Agency</i> right to object to transfers or licensing.....	48
30.4 Consequences of non-compliance.....	49
ARTICLE 31 — ACCESS RIGHTS TO RESULTS.....	49
31.1 Exercise of access rights — Waiving of access rights — No sub-licensing.....	49
31.2 Access rights for other beneficiaries, for implementing their own tasks under the action.....	49
31.3 Access rights for other beneficiaries, for exploiting their own results.....	49
31.4 Access rights of affiliated entities.....	50
31.5 Access rights for the EU institutions, bodies, offices or agencies and EU Member States.....	50
31.6 Access rights for third parties.....	50
31.7 Consequences of non-compliance.....	50
SECTION 4 OTHER RIGHTS AND OBLIGATIONS.....	50
ARTICLE 32 — RECRUITMENT AND WORKING CONDITIONS FOR RESEARCHERS.....	51
32.1 Obligation to take measures to implement the European Charter for Researchers and Code of Conduct for the Recruitment of Researchers.....	51
32.2 Consequences of non-compliance.....	51
ARTICLE 33 — GENDER EQUALITY.....	51
33.1 Obligation to aim for gender equality.....	51
33.2 Consequences of non-compliance.....	51
ARTICLE 34 — ETHICS.....	51
34.1 Obligation to comply with ethical principles.....	51
34.2 Activities raising ethical issues.....	52
34.3 Activities involving human embryos or human embryonic stem cells.....	52
34.4 Consequences of non-compliance.....	52
ARTICLE 35 — CONFLICT OF INTERESTS.....	53
35.1 Obligation to avoid a conflict of interests.....	53
35.2 Consequences of non-compliance.....	53

ARTICLE 36 — CONFIDENTIALITY.....	53
36.1 General obligation to maintain confidentiality.....	53
36.2 Consequences of non-compliance.....	54
ARTICLE 37 — SECURITY-RELATED OBLIGATIONS.....	54
37.1 Results with a security recommendation.....	54
37.2 Classified results.....	54
37.3 Activities involving dual-use goods or dangerous materials and substances.....	54
37.4 Consequences of non-compliance.....	54
ARTICLE 38 — PROMOTING THE ACTION — VISIBILITY OF EU FUNDING.....	55
38.1 Communication activities by beneficiaries.....	55
38.2 Communication activities by the <i>Agency</i>	55
38.3 Consequences of non-compliance.....	57
ARTICLE 39 — PROCESSING OF PERSONAL DATA.....	57
39.1 Processing of personal data by the <i>Agency and the Commission</i>	57
39.2 Processing of personal data by the beneficiaries.....	57
39.3 Consequences of non-compliance.....	57
ARTICLE 40 — ASSIGNMENTS OF CLAIMS FOR PAYMENT AGAINST THE <i>AGENCY</i>	58
CHAPTER 5 DIVISION OF BENEFICIARIES' ROLES AND RESPONSIBILITIES	58
ARTICLE 41 — DIVISION OF BENEFICIARIES' ROLES AND RESPONSIBILITIES	58
41.1 Roles and responsibilities towards the <i>Agency</i>	58
41.2 Internal division of roles and responsibilities.....	58
41.3 Internal arrangements between beneficiaries — Consortium agreement.....	59
41.4 Relationship with complementary beneficiaries — Collaboration agreement.....	60
41.5 Relationship with partners of a joint action — Coordination agreement.....	60
CHAPTER 6 REJECTION OF COSTS — REDUCTION OF THE GRANT — RECOVERY — PENALTIES — DAMAGES — SUSPENSION — TERMINATION — FORCE MAJEURE.....	60
SECTION 1 REJECTION OF COSTS — REDUCTION OF THE GRANT — RECOVERY — PENALTIES.....	60
ARTICLE 42 — REJECTION OF INELIGIBLE COSTS.....	60
42.1 Conditions.....	60
42.2 Ineligible costs to be rejected — Calculation — Procedure.....	60
42.3 Effects.....	60
ARTICLE 43 — REDUCTION OF THE GRANT.....	61
43.1 Conditions.....	61
43.2 Amount to be reduced — Calculation — Procedure.....	61

43.3 Effects.....	61
ARTICLE 44 — RECOVERY OF UNDUE AMOUNTS.....	61
44.1 Amount to be recovered — Calculation — Procedure.....	61
ARTICLE 45 — ADMINISTRATIVE AND FINANCIAL PENALTIES.....	65
45.1 Conditions.....	65
45.2 Duration — Amount of penalty — Calculation.....	66
45.3 Procedure.....	66
SECTION 2 LIABILITY FOR DAMAGES.....	67
ARTICLE 46 — LIABILITY FOR DAMAGES.....	67
46.1 Liability of the <i>Agency</i>	67
46.2 Liability of the beneficiaries.....	67
SECTION 3 SUSPENSION AND TERMINATION.....	68
ARTICLE 47 — SUSPENSION OF PAYMENT DEADLINE.....	68
47.1 Conditions.....	68
47.2 Procedure.....	68
ARTICLE 48 — SUSPENSION OF PAYMENTS.....	69
48.1 Conditions.....	69
48.2 Procedure.....	69
ARTICLE 49 — SUSPENSION OF THE ACTION IMPLEMENTATION.....	69
49.1 Suspension of the action implementation, by the beneficiaries.....	69
49.2 Suspension of the action implementation, by the <i>Agency</i>	70
ARTICLE 50 — TERMINATION OF THE AGREEMENT OR OF THE PARTICIPATION OF ONE OR MORE BENEFICIARIES.....	71
50.1 Termination of the Agreement by the beneficiaries.....	71
50.2 Termination of the participation of one or more beneficiaries, by the beneficiaries.....	72
50.3 Termination of the Agreement or the participation of one or more beneficiaries, by the <i>Agency</i> ... 74	
SECTION 4 FORCE MAJEURE.....	78
ARTICLE 51 — FORCE MAJEURE.....	78
CHAPTER 7 FINAL PROVISIONS.....	78
ARTICLE 52 — COMMUNICATIONS BETWEEN THE PARTIES.....	78
52.1 Form and means of communication.....	78
52.2 Date of communication.....	79
52.3 Addresses for communication.....	79
ARTICLE 53 — INTERPRETATION OF THE AGREEMENT.....	80
53.1 Precedence of the Terms and Conditions over the Annexes.....	80

53.2 Privileges and immunities.....	80
ARTICLE 54 — CALCULATION OF PERIODS, DATES AND DEADLINES.....	80
ARTICLE 55 — AMENDMENTS TO THE AGREEMENT.....	80
55.1 Conditions.....	80
55.2 Procedure.....	80
ARTICLE 56 — ACCESSION TO THE AGREEMENT.....	81
56.1 Accession of the beneficiaries mentioned in the Preamble.....	81
56.2 Addition of new beneficiaries.....	81
ARTICLE 57 — APPLICABLE LAW AND SETTLEMENT OF DISPUTES.....	81
57.1 Applicable law.....	81
57.2 Dispute settlement.....	81
ARTICLE 58 — ENTRY INTO FORCE OF THE AGREEMENT.....	82

CHAPTER 1 GENERAL

ARTICLE 1 — SUBJECT OF THE AGREEMENT

This Agreement sets out the rights and obligations and the terms and conditions applicable to the grant awarded to the beneficiaries for implementing the action set out in Chapter 2.

CHAPTER 2 ACTION

ARTICLE 2 — ACTION TO BE IMPLEMENTED

The grant is awarded for the action entitled '*Intelligent Portable ContROl SyStem — iCROSS*' ('**action**'), as described in Annex 1.

ARTICLE 3 — DURATION AND STARTING DATE OF THE ACTION

The duration of the action will be **36 months** as of *1 September 2016* ('**starting date of the action**').

ARTICLE 4 — ESTIMATED BUDGET AND BUDGET TRANSFERS

4.1 Estimated budget

The '**estimated budget**' for the action is set out in Annex 2.

It contains the estimated eligible costs and the forms of costs, broken down by beneficiary and budget category (see Articles 5, 6).

4.2 Budget transfers

The estimated budget breakdown indicated in Annex 2 may be adjusted by transfers of amounts between beneficiaries or between budget categories (or both). This does not require an amendment according to Article 55, if the action is implemented as described in Annex 1.

However, the beneficiaries may not add costs relating to subcontracts not provided for in Annex 1, unless such additional subcontracts are approved by an amendment or in accordance with Article 13.

CHAPTER 3 GRANT

ARTICLE 5 — GRANT AMOUNT, FORM OF GRANT, REIMBURSEMENT RATES AND FORMS OF COSTS

5.1 Maximum grant amount

The '**maximum grant amount**' is **EUR 4,501,877.50** (four million five hundred and one thousand eight hundred and seventy seven EURO and fifty eurocents).

5.2 Form of grant, reimbursement rates and forms of costs

The grant reimburses **100% of the action's eligible costs** (see Article 6) (**'reimbursement of eligible costs grant'**) (see Annex 2).

The estimated eligible costs of the action are EUR [REDACTED]

Eligible costs (see Article 6) must be declared under the following forms (**'forms of costs'**):

(a) for **direct personnel costs**:

- as actually incurred costs (**'actual costs'**) or
- on the basis of an amount per unit calculated by the beneficiary in accordance with its usual cost accounting practices (**'unit costs'**).

Personnel **costs for SME owners or beneficiaries that are natural persons** not receiving a salary (see Article 6.2, Points A.4 and A.5) must be declared on the basis of the amount per unit set out in Annex 2 (**'unit costs'**);

(b) for **direct costs for subcontracting**: as actually incurred costs (**'actual costs'**);

(c) for **direct costs of providing financial support to third parties**: *not applicable*;

(d) for **other direct costs**: as actually incurred costs (**'actual costs'**);

(e) for **indirect costs**: on the basis of a flat-rate applied as set out in Article 6.2, Point E (**'flat-rate costs'**);

(f) *specific cost category(ies): not applicable.*

5.3 Final grant amount — Calculation

The **'final grant amount'** depends on the actual extent to which the action is implemented in accordance with the Agreement's terms and conditions.

This amount is calculated by the *Agency* — when the payment of the balance is made (see Article 21.4) — in the following steps:

Step 1 – Application of the reimbursement rates to the eligible costs

Step 2 – Limit to the maximum grant amount

Step 3 – Reduction due to the no-profit rule

Step 4 – Reduction due to improper implementation or breach of other obligations

5.3.1 Step 1 — Application of the reimbursement rates to the eligible costs

The reimbursement rate(s) (see Article 5.2) are applied to the eligible costs (actual costs, unit costs and flat-rate costs; see Article 6) declared by the beneficiaries (see Article 20) and approved by the *Agency* (see Article 21).

5.3.2 Step 2 — Limit to the maximum grant amount

If the amount obtained following Step 1 is higher than the maximum grant amount set out in Article 5.1, it will be limited to the latter.

5.3.3 Step 3 — Reduction due to the no-profit rule

The grant must not produce a profit.

‘**Profit**’ means the surplus of the amount obtained following Steps 1 and 2 plus the action’s total receipts, over the action’s total eligible costs.

The ‘**action’s total eligible costs**’ are the consolidated total eligible costs approved by the *Agency*.

The ‘**action’s total receipts**’ are the consolidated total receipts generated during its duration (see Article 3).

The following are considered **receipts**:

- (a) income generated by the action; if the income is generated from selling equipment or other assets purchased under the Agreement, the receipt is up to the amount declared as eligible under the Agreement;
- (b) financial contributions given by third parties to the beneficiary specifically to be used for the action, and
- (c) in-kind contributions provided by third parties free of charge and specifically to be used for the action, if they have been declared as eligible costs.

The following are however not considered receipts:

- (a) income generated by exploiting the action’s results (see Article 28);
- (b) financial contributions by third parties, if they may be used to cover costs other than the eligible costs (see Article 6);
- (c) financial contributions by third parties with no obligation to repay any amount unused at the end of the period set out in Article 3.

If there is a profit, it will be deducted from the amount obtained following Steps 1 and 2.

5.3.4 Step 4 — Reduction due to improper implementation or breach of other obligations — Reduced grant amount — Calculation

If the grant is reduced (see Article 43), the *Agency* will calculate the reduced grant amount by deducting the amount of the reduction (calculated in proportion to the improper implementation of the action or to the seriousness of the breach of obligations in accordance with Article 43.2) from the maximum grant amount set out in Article 5.1.

The final grant amount will be the lower of the following two:

- the amount obtained following Steps 1 to 3 or
- the reduced grant amount following Step 4.

5.4 Revised final grant amount — Calculation

If — after the payment of the balance (in particular, after checks, reviews, audits or investigations; see Article 22) — the *Agency* rejects costs (see Article 42) or reduces the grant (see Article 43), it will calculate the ‘**revised final grant amount**’ for the beneficiary concerned by the findings.

This amount is calculated by the *Agency* on the basis of the findings, as follows:

- in case of **rejection of costs**: by applying the reimbursement rate to the revised eligible costs approved by the *Agency* for the beneficiary concerned;
- in case of **reduction of the grant**: by calculating the concerned beneficiary’s share in the grant amount reduced in proportion to its improper implementation of the action or to the seriousness of its breach of obligations (see Article 43.2).

In case of **rejection of costs and reduction of the grant**, the revised final grant amount for the beneficiary concerned will be the lower of the two amounts above.

ARTICLE 6 — ELIGIBLE AND INELIGIBLE COSTS

6.1 General conditions for costs to be eligible

‘**Eligible costs**’ are costs that meet the following criteria:

(a) for **actual costs**:

- (i) they must be actually incurred by the beneficiary;
- (ii) they must be incurred in the period set out in Article 3, with the exception of costs relating to the submission of the periodic report for the last reporting period and the final report (see Article 20);
- (iii) they must be indicated in the estimated budget set out in Annex 2;
- (iv) they must be incurred in connection with the action as described in Annex 1 and necessary for its implementation;
- (v) they must be identifiable and verifiable, in particular recorded in the beneficiary’s accounts in accordance with the accounting standards applicable in the country where the beneficiary is established and with the beneficiary’s usual cost accounting practices;
- (vi) they must comply with the applicable national law on taxes, labour and social security, and
- (vii) they must be reasonable, justified and must comply with the principle of sound financial management, in particular regarding economy and efficiency;

(b) for **unit costs**:

(i) they must be calculated as follows:

{amounts per unit set out in Annex 2 or calculated by the beneficiary in accordance with its usual cost accounting practices (see Article 6.2, Point A)}

multiplied by

the number of actual units};

(ii) the number of actual units must comply with the following conditions:

- the units must be actually used or produced in the period set out in Article 3;
- the units must be necessary for implementing the action or produced by it, and
- the number of units must be identifiable and verifiable, in particular supported by records and documentation (see Article 18);

(c) for **flat-rate costs**:

(i) they must be calculated by applying the flat-rate set out in Annex 2, and

(ii) the costs (actual costs or unit costs) to which the flat-rate is applied must comply with the conditions for eligibility set out in this Article.

6.2 Specific conditions for costs to be eligible

Costs are eligible if they comply with the general conditions (see above) and the specific conditions set out below for each of the following budget categories:

- A. direct personnel costs;
- B. direct costs of subcontracting;
- C. *not applicable*;
- D. other direct costs;
- E. indirect costs;
- F. *not applicable*.

‘Direct costs’ are costs that are directly linked to the action implementation and can therefore be attributed to it directly. They must not include any indirect costs (see Point E below).

‘Indirect costs’ are costs that are not directly linked to the action implementation and therefore cannot be attributed directly to it.

A. Direct personnel costs

Types of eligible personnel costs

A.1 **Personnel costs** are eligible, if they are related to personnel working for the beneficiary under an employment contract (or equivalent appointing act) and assigned to the action (**‘costs for employees (or equivalent)’**). They must be limited to salaries (including during parental leave), social security contributions, taxes and other costs included in the **remuneration**, if they arise from national law or the employment contract (or equivalent appointing act).

Beneficiaries that are non-profit legal entities² may also declare as personnel costs **additional remuneration** for personnel assigned to the action (including payments on the basis of supplementary contracts regardless of their nature), if:

- (a) it is part of the beneficiary's usual remuneration practices and is paid in a consistent manner whenever the same kind of work or expertise is required;
- (b) the criteria used to calculate the supplementary payments are objective and generally applied by the beneficiary, regardless of the source of funding used.

Additional remuneration for personnel assigned to the action is eligible up to the following amount:

- (a) if the person works full time and exclusively on the action during the full year: up to EUR 8 000;
- (b) if the person works exclusively on the action but not full-time or not for the full year: up to the corresponding pro-rata amount of EUR 8 000, or
- (c) if the person does not work exclusively on the action: up to a pro-rata amount calculated as follows:

{EUR 8 000

divided by

the number of annual productive hours (see below)},

multiplied by

the number of hours that the person has worked on the action during the year}.

A.2 The **costs for natural persons working under a direct contract** with the beneficiary other than an employment contract are eligible personnel costs, if:

- (a) the person works under the beneficiary's instructions and, unless otherwise agreed with the beneficiary, on the beneficiary's premises;
- (b) the result of the work carried out belongs to the beneficiary, and
- (c) the costs are not significantly different from those for personnel performing similar tasks under an employment contract with the beneficiary.

A.3 The **costs of personnel seconded by a third party against payment** are eligible personnel costs, if the conditions in Article 11.1 are met.

² For the definition, see Article 2.1(14) of the Rules for Participation Regulation No 1290/2013: '**non-profit legal entity**' means a legal entity which by its legal form is non-profit-making or which has a legal or statutory obligation not to distribute profits to its shareholders or individual members.

A.4 **Costs of owners** of beneficiaries that are small and medium-sized enterprises (**‘SME owners’**) who are working on the action and who do not receive a salary are eligible personnel costs, if they correspond to the amount per unit set out in Annex 2 multiplied by the number of actual hours worked on the action.

A.5 **Costs of ‘beneficiaries that are natural persons’** not receiving a salary are eligible personnel costs, if they correspond to the amount per unit set out in Annex 2 multiplied by the number of actual hours worked on the action.

Calculation

Personnel costs must be calculated by the beneficiaries as follows:

{ hourly rate
multiplied by
the number of actual hours worked on the action},
plus
for non-profit legal entities: additional remuneration to personnel assigned to the action under the conditions set out above (Point A.1)).

The number of actual hours declared for a person must be identifiable and verifiable (see Article 18).

The total number of hours declared in EU or Euratom grants, for a person for a year, cannot be higher than the annual productive hours used for the calculations of the hourly rate. Therefore, the maximum number of hours that can be declared for the grant is:

{the number of annual productive hours for the year (see below)
minus
total number of hours declared by the beneficiary for that person in that year for other EU or Euratom grants}.

The **‘hourly rate’** is one of the following:

(a) for personnel costs declared as **actual costs**: the hourly rate is the amount calculated as follows:

{actual annual personnel costs (excluding additional remuneration) for the person
divided by
number of annual productive hours}.

The beneficiaries must use the annual personnel costs and the number of annual productive hours for each financial year covered by the reporting period. If a financial year is not closed at the end of the reporting period, the beneficiaries must use the hourly rate of the last closed financial year available.

For the ‘number of annual productive hours’, the beneficiaries may choose one of the following:

(i) ‘fixed number of hours’: 1 720 hours for persons working full time (or corresponding pro-rata for persons not working full time);

- (ii) ‘individual annual productive hours’: the total number of hours worked by the person in the year for the beneficiary, calculated as follows:

{annual workable hours of the person (according to the employment contract, applicable collective labour agreement or national law)

plus

overtime worked

minus

absences (such as sick leave and special leave)}.

‘Annual workable hours’ means the period during which the personnel must be working, at the employer’s disposal and carrying out his/her activity or duties under the employment contract, applicable collective labour agreement or national working time legislation.

If the contract (or applicable collective labour agreement or national working time legislation) does not allow to determine the annual workable hours, this option cannot be used;

- (iii) ‘standard annual productive hours’: the ‘standard number of annual hours’ generally applied by the beneficiary for its personnel in accordance with its usual cost accounting practices. This number must be at least 90% of the ‘standard annual workable hours’.

If there is no applicable reference for the standard annual workable hours, this option cannot be used.

For all options, the actual time spent on **parental leave** by a person assigned to the action may be deducted from the number of annual productive hours;

- (b) for personnel costs declared on the basis of **unit costs**: the hourly rate is one of the following:

- (i) for SME owners or beneficiaries that are natural persons: the hourly rate set out in Annex 2 (see Points A.4 and A.5 above), or
- (ii) for personnel costs declared on the basis of the beneficiary’s usual cost accounting practices: the hourly rate calculated by the beneficiary in accordance with its usual cost accounting practices, if:
 - the cost accounting practices used are applied in a consistent manner, based on objective criteria, regardless of the source of funding;
 - the hourly rate is calculated using the actual personnel costs recorded in the beneficiary’s accounts, excluding any ineligible cost or costs included in other budget categories.

The actual personnel costs may be adjusted by the beneficiary on the basis of budgeted or estimated elements. Those elements must be relevant for calculating

the personnel costs, reasonable and correspond to objective and verifiable information;

and

- the hourly rate is calculated using the number of annual productive hours (see above).

B. Direct costs of subcontracting (including related duties, taxes and charges such as non-deductible value added tax (VAT) paid by the beneficiary) are eligible if the conditions in Article 13.1.1 are met.

C. Direct costs of providing financial support to third parties *not applicable*.

D. Other direct costs

D.1 Travel costs and related subsistence allowances (including related duties, taxes and charges such as non-deductible value added tax (VAT) paid by the beneficiary) are eligible if they are in line with the beneficiary's usual practices on travel.

D.2 The depreciation costs of equipment, infrastructure or other assets *(new or second-hand) as recorded in the beneficiary's accounts are eligible, if they were purchased in accordance with Article 10.1.1 and written off in accordance with international accounting standards and the beneficiary's usual accounting practices.*

The costs of renting or leasing equipment, infrastructure or other assets (including related duties, taxes and charges such as non-deductible value added tax (VAT) paid by the beneficiary) are also eligible, if they do not exceed the depreciation costs of similar equipment, infrastructure or assets and do not include any financing fees.

*The costs of equipment, infrastructure or other assets **contributed in-kind against payment** are eligible, if they do not exceed the depreciation costs of similar equipment, infrastructure or assets, do not include any financing fees and if the conditions in Article 11.1 are met.*

The only portion of the costs that will be taken into account is that which corresponds to the duration of the action and rate of actual use for the purposes of the action.

D.3 Costs of other goods and services (including related duties, taxes and charges such as non-deductible value added tax (VAT) paid by the beneficiary) are eligible, if they are:

- (a) purchased specifically for the action and in accordance with Article 10.1.1 or
- (b) contributed in kind against payment and in accordance with Article 11.1.

Such goods and services include, for instance, consumables and supplies, dissemination (including open access), protection of results, certificates on the financial statements (if they are required by the Agreement), certificates on the methodology, translations and publications.

D.4 Capitalised and operating costs of ‘large research infrastructure’³ directly used for the action are eligible, if:

- (a) the value of the large research infrastructure represents at least 75% of the total fixed assets (at historical value in its last closed balance sheet before the date of the signature of the Agreement or as determined on the basis of the rental and leasing costs of the research infrastructure⁴);*
- (b) the beneficiary’s methodology for declaring the costs for large research infrastructure has been positively assessed by the Commission (‘ex-ante assessment’);*
- (c) the beneficiary declares as direct eligible costs only the portion which corresponds to the duration of the action and the rate of actual use for the purposes of the action, and*
- (d) they comply with the conditions as further detailed in the annotations to the H2020 grant agreements.*

E. Indirect costs

Indirect costs are eligible if they are declared on the basis of the flat-rate of 25% of the eligible direct costs (see Article 5.2 and Points A to D above), from which are excluded:

- (a) costs of subcontracting and
- (b) costs of in-kind contributions provided by third parties which are not used on the beneficiary’s premises;
- (c) *not applicable*;
- (d) *not applicable*.

Beneficiaries receiving an operating grant⁵ financed by the EU or Euratom budget cannot declare indirect costs for the period covered by the operating grant.

³ ‘**Large research infrastructure**’ means research infrastructure of a total value of at least EUR 20 million, for a beneficiary, calculated as the sum of historical asset values of each individual research infrastructure of that beneficiary, as they appear in its last closed balance sheet before the date of the signature of the Agreement or as determined on the basis of the rental and leasing costs of the research infrastructure.

⁴ For the definition, see Article 2(6) of Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) (OJ L 347, 20.12.2013 p.104)-(**‘Horizon 2020 Framework Programme Regulation No 1291/2013’**): ‘**Research infrastructure**’ are facilities, resources and services that are used by the research communities to conduct research and foster innovation in their fields. Where relevant, they may be used beyond research, e.g. for education or public services. They include: major scientific equipment (or sets of instruments); knowledge-based resources such as collections, archives or scientific data; e-infrastructures such as data and computing systems and communication networks; and any other infrastructure of a unique nature essential to achieve excellence in research and innovation. Such infrastructures may be ‘single-sited’, ‘virtual’ or ‘distributed’.

⁵ For the definition, see Article 121(1)(b) of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 218, 26.10.2012, p.1) (**‘Financial Regulation No 966/2012’**): ‘**operating grant**’ means direct financial contribution, by way of donation, from the budget in order to finance the functioning of a body which pursues an aim of general EU interest or has an objective forming part of and supporting an EU policy.

F. Specific cost category(ies)

Not applicable

6.3 Conditions for costs of linked third parties to be eligible

not applicable

6.4 Conditions for in-kind contributions provided by third parties free of charge to be eligible

In-kind contributions provided free of charge are eligible direct costs (for the beneficiary), if the costs incurred by the third party fulfil — *mutatis mutandis* — the general and specific conditions for eligibility set out in this Article (Article 6.1 and 6.2) and Article 12.1.

6.5 Ineligible costs

‘**Ineligible costs**’ are:

(a) costs that do not comply with the conditions set out above (Article 6.1 to 6.4), in particular:

- (i) costs related to return on capital;
- (ii) debt and debt service charges;
- (iii) provisions for future losses or debts;
- (iv) interest owed;
- (v) doubtful debts;
- (vi) currency exchange losses;
- (vii) bank costs charged by the beneficiary’s bank for transfers from the *Agency*;
- (viii) excessive or reckless expenditure;
- (ix) deductible VAT;
- (x) costs incurred during suspension of the implementation of the action (see Article 49);

(b) costs declared under another EU or Euratom grant (including grants awarded by a Member State and financed by the EU or Euratom budget and grants awarded by bodies other than the *Agency* for the purpose of implementing the EU or Euratom budget); in particular, indirect costs if the beneficiary is already receiving an operating grant financed by the EU or Euratom budget in the same period.

6.6 Consequences of declaration of ineligible costs

Declared costs that are ineligible will be rejected (see Article 42).

This may also lead to any of the other measures described in Chapter 6.

**CHAPTER 4 RIGHTS AND OBLIGATIONS OF THE PARTIES****SECTION 1 RIGHTS AND OBLIGATIONS RELATED TO IMPLEMENTING THE ACTION****ARTICLE 7 — GENERAL OBLIGATION TO PROPERLY IMPLEMENT THE ACTION****7.1 General obligation to properly implement the action**

The beneficiaries must implement the action as described in Annex 1 and in compliance with the provisions of the Agreement and all legal obligations under applicable EU, international and national law.

7.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 8 — RESOURCES TO IMPLEMENT THE ACTION — THIRD PARTIES INVOLVED IN THE ACTION

The beneficiaries must have the appropriate resources to implement the action.

If it is necessary to implement the action, the beneficiaries may:

- purchase goods, works and services (see Article 10);
- use in-kind contributions provided by third parties against payment (see Article 11);
- use in-kind contributions provided by third parties free of charge (see Article 12);
- call upon subcontractors to implement action tasks described in Annex 1 (see Article 13);
- call upon linked third parties to implement action tasks described in Annex 1 (see Article 14).

In these cases, the beneficiaries retain sole responsibility towards the *Agency* and the other beneficiaries for implementing the action.

ARTICLE 9 — IMPLEMENTATION OF ACTION TASKS BY BENEFICIARIES NOT RECEIVING EU FUNDING

Not applicable

ARTICLE 10 — PURCHASE OF GOODS, WORKS OR SERVICES**10.1 Rules for purchasing goods, works or services**

10.1.1 If necessary to implement the action, the beneficiaries may purchase goods, works or services.

The beneficiaries must make such purchases ensuring the best value for money or, if appropriate, the lowest price. In doing so, they must avoid any conflict of interests (see Article 35).

The beneficiaries must ensure that *the Agency*, the Commission, the European Court of Auditors (ECA) and the European Anti-Fraud Office (OLAF) can exercise their rights under Articles 22 and 23 also towards their contractors.

10.1.2 Beneficiaries that are ‘contracting authorities’ within the meaning of Directive 2004/18/EC⁶ or ‘contracting entities’ within the meaning of Directive 2004/17/EC⁷ must comply with the applicable national law on public procurement.

10.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under Article 10.1.1, the costs related to the contract concerned will be ineligible (see Article 6) and will be rejected (see Article 42).

If a beneficiary breaches any of its obligations under Article 10.1.2, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 11 — USE OF IN-KIND CONTRIBUTIONS PROVIDED BY THIRD PARTIES AGAINST PAYMENT

11.1 Rules for the use of in-kind contributions against payment

If necessary to implement the action, the beneficiaries may use in-kind contributions provided by third parties against payment.

The beneficiaries may declare costs related to the payment of in-kind contributions as eligible (see Article 6.1 and 6.2), up to the third parties’ costs for the seconded persons, contributed equipment, infrastructure or other assets or other contributed goods and services.

The third parties and their contributions must be set out in Annex 1. The *Agency* may however approve in-kind contributions not set out in Annex 1 without amendment (see Article 55), if:

- they are specifically justified in the periodic technical report and
- their use does not entail changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

The beneficiaries must ensure that *the Agency*, the Commission, the European Court of Auditors (ECA) and the European Anti-Fraud Office (OLAF) can exercise their rights under Articles 22 and 23 also towards the third parties.

⁶ Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public work contracts, public supply contracts and public service contracts (OJ L 134, 30.04.2004, p. 114).

⁷ Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors (OJ L 134, 30.04.2004, p. 1).

11.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the costs related to the payment of the in-kind contribution will be ineligible (see Article 6) and will be rejected (see Article 42).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 12 — USE OF IN-KIND CONTRIBUTIONS PROVIDED BY THIRD PARTIES FREE OF CHARGE

12.1 Rules for the use of in-kind contributions free of charge

If necessary to implement the action, the beneficiaries may use in-kind contributions provided by third parties free of charge.

The beneficiaries may declare costs incurred by the third parties for the seconded persons, contributed equipment, infrastructure or other assets or other contributed goods and services as eligible in accordance with Article 6.4.

The third parties and their contributions must be set out in Annex 1. The *Agency* may however approve in-kind contributions not set out in Annex 1 without amendment (see Article 55), if:

- they are specifically justified in the periodic technical report and
- their use does not entail changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

The beneficiaries must ensure that *the Agency*, the Commission, the European Court of Auditors (ECA) and the European Anti-Fraud Office (OLAF) can exercise their rights under Articles 22 and 23 also towards the third parties.

12.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the costs incurred by the third parties related to the in-kind contribution will be ineligible (see Article 6) and will be rejected (see Article 42).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 13 — IMPLEMENTATION OF ACTION TASKS BY SUBCONTRACTORS

13.1 Rules for subcontracting action tasks

13.1.1 If necessary to implement the action, the beneficiaries may award subcontracts covering the implementation of certain action tasks described in Annex 1.

Subcontracting may cover only a limited part of the action.

The beneficiaries must award the subcontracts ensuring the best value for money or, if appropriate, the lowest price. In doing so, they must avoid any conflict of interests (see Article 35).

The tasks to be implemented and the estimated cost for each subcontract must be set out in Annex 1 and the total estimated costs of subcontracting per beneficiary must be set out in Annex 2. The

Agency may however approve subcontracts not set out in Annex 1 and 2 without amendment (see Article 55), if:

- they are specifically justified in the periodic technical report and
- they do not entail changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

The beneficiaries must ensure that *the Agency*, the Commission, the European Court of Auditors (ECA) and the European Anti-Fraud Office (OLAF) can exercise their rights under Articles 22 and 23 also towards their subcontractors.

13.1.2 The beneficiaries must ensure that their obligations under Articles 35, 36, 38 and 46 also apply to the subcontractors.

Beneficiaries that are ‘contracting authorities’ within the meaning of Directive 2004/18/EC or ‘contracting entities’ within the meaning of Directive 2004/17/EC must comply with the applicable national law on public procurement.

13.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under Article 13.1.1, the costs related to the subcontract concerned will be ineligible (see Article 6) and will be rejected (see Article 42).

If a beneficiary breaches any of its obligations under Article 13.1.2, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 14 — IMPLEMENTATION OF ACTION TASKS BY LINKED THIRD PARTIES

Not applicable

ARTICLE 15 — FINANCIAL SUPPORT TO THIRD PARTIES

15.1 Rules for providing financial support to third parties

Not applicable

15.2 Financial support in the form of prizes

Not applicable

15.3 Consequences of non-compliance

Not applicable

ARTICLE 16 — PROVISION OF TRANS-NATIONAL OR VIRTUAL ACCESS TO RESEARCH INFRASTRUCTURE

16.1 Rules for providing trans-national access to research infrastructure

Not applicable

16.2 Rules for providing virtual access to research infrastructure

Not applicable

16.3 Consequences of non-compliance

Not applicable

SECTION 2 RIGHTS AND OBLIGATIONS RELATED TO THE GRANT ADMINISTRATION

ARTICLE 17 — GENERAL OBLIGATION TO INFORM

17.1 General obligation to provide information upon request

The beneficiaries must provide — during implementation of the action or afterwards and in accordance with Article 41.2 — any information requested in order to verify eligibility of the costs, proper implementation of the action and compliance with any other obligation under the Agreement.

17.2 Obligation to keep information up to date and to inform about events and circumstances likely to affect the Agreement

Each beneficiary must keep information stored in the 'Beneficiary Register' (via the electronic exchange system; see Article 52) up to date, in particular, its name, address, legal representatives, legal form and organisation type.

Each beneficiary must immediately inform the coordinator — which must immediately inform the *Agency* and the other beneficiaries — of any of the following:

- (a) **events** which are likely to affect significantly or delay the implementation of the action or the EU's financial interests, in particular:
 - (i) changes in its legal, financial, technical, organisational or ownership situation
- (b) **circumstances** affecting:
 - (i) the decision to award the grant or
 - (ii) compliance with requirements under the Agreement.

17.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 18 — KEEPING RECORDS — SUPPORTING DOCUMENTATION

18.1 Obligation to keep records and other supporting documentation

The beneficiaries must — for a period of *five* years after the payment of the balance — keep records and other supporting documentation in order to prove the proper implementation of the action and the costs they declare as eligible.

They must make them available upon request (see Article 17) or in the context of checks, reviews, audits or investigations (see Article 22).

If there are on-going checks, reviews, audits, investigations, litigation or other pursuits of claims under the Agreement (including the extension of findings; see Articles 22), the beneficiaries must keep the records and other supporting documentation until the end of these procedures.

The beneficiaries must keep the original documents. Digital and digitalised documents are considered originals if they are authorised by the applicable national law. The *Agency* may accept non-original documents if it considers that they offer a comparable level of assurance.

18.1.1 Records and other supporting documentation on the scientific and technical implementation

The beneficiaries must keep records and other supporting documentation on scientific and technical implementation of the action in line with the accepted standards in the respective field.

18.1.2 Records and other documentation to support the costs declared

The beneficiaries must keep the records and documentation supporting the costs declared, in particular the following:

- (a) for **actual costs**: adequate records and other supporting documentation to prove the costs declared, such as contracts, subcontracts, invoices and accounting records. In addition, the beneficiaries' usual cost accounting practices and internal control procedures must enable direct reconciliation between the amounts declared, the amounts recorded in their accounts and the amounts stated in the supporting documentation;
- (b) for **unit costs**: adequate records and other supporting documentation to prove the number of units declared. Beneficiaries do not need to identify the actual eligible costs covered or to keep or provide supporting documentation (such as accounting statements) to prove the amount per unit.

In addition, for **direct personnel costs declared as unit costs calculated in accordance with the beneficiary's usual cost accounting practices**, the beneficiaries must keep adequate

records and documentation to prove that the cost accounting practices used comply with the conditions set out in Article 6.2, Point A.

The beneficiaries may submit to the Commission, for approval, a certificate (drawn up in accordance with Annex 6) stating that their usual cost accounting practices comply with these conditions (**‘certificate on the methodology’**). If the certificate is approved, costs declared in line with this methodology will not be challenged subsequently, unless the beneficiaries have concealed information for the purpose of the approval.

- (c) for **flat-rate costs**: adequate records and other supporting documentation to prove the eligibility of the costs to which the flat-rate is applied. The beneficiaries do not need to identify the costs covered or provide supporting documentation (such as accounting statements) to prove the amount declared at a flat-rate.

In addition, for **personnel costs** (declared as actual costs or on the basis of unit costs), the beneficiaries must keep **time records** for the number of hours declared. The time records must be in writing and approved by the persons working on the action and their supervisors, at least monthly. In the absence of reliable time records of the hours worked on the action, the *Agency* may accept alternative evidence supporting the number of hours declared, if it considers that it offers an adequate level of assurance.

As an exception, for **persons working exclusively on the action**, there is no need to keep time records, if the beneficiary signs a **declaration** confirming that the persons concerned have worked exclusively on the action.

18.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, costs insufficiently substantiated will be ineligible (see Article 6) and will be rejected (see Article 42), and the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 19 — SUBMISSION OF DELIVERABLES

19.1 Obligation to submit deliverables

The coordinator must submit the **‘deliverables’** identified in Annex 1, in accordance with the timing and conditions set out in it.

19.2 Consequences of non-compliance

If the coordinator breaches any of its obligations under this Article, the *Agency* may apply any of the measures described in Chapter 6.

ARTICLE 20 — REPORTING — PAYMENT REQUESTS

20.1 Obligation to submit reports

The coordinator must submit to the *Agency* (see Article 52) the technical and financial reports set out in this Article. These reports include requests for payment and must be drawn up using the forms and templates provided in the electronic exchange system (see Article 52).

20.2 Reporting periods

The action is divided into the following ‘**reporting periods**’:

- RP1: from month 1 to month 18
- RP2: *from month 19 to month 36*

20.3 Periodic reports — Requests for interim payments

The coordinator must submit a periodic report within 60 days following the end of each reporting period.

The **periodic report** must include the following:

(a) a ‘**periodic technical report**’ containing:

- (i) an **explanation of the work carried out** by the beneficiaries;
- (ii) an **overview of the progress** towards the objectives of the action, including milestones and deliverables identified in Annex 1.

This report must include explanations justifying the differences between work expected to be carried out in accordance with Annex 1 and that actually carried out.

The report must also detail the exploitation and dissemination of the results and — if required in Annex 1 — an updated ‘**plan for the exploitation and dissemination of the results**’;

- (iii) a **summary** for publication by the *Agency*;
- (iv) the answers to the ‘**questionnaire**’, covering issues related to the action implementation and the economic and societal impact, notably in the context of the Horizon 2020 key performance indicators and the Horizon 2020 monitoring requirements;

(b) a ‘**periodic financial report**’ containing:

- (i) an ‘**individual financial statement**’ (see Annex 4) from each beneficiary, for the reporting period concerned.

The individual financial statement must detail the eligible costs (actual costs, unit costs and flat-rate costs; see Article 6) for each budget category (see Annex 2).

The beneficiaries must declare all eligible costs, even if — for actual costs, unit costs and flat-rate costs — they exceed the amounts indicated in the estimated budget (see Annex 2). Amounts which are not declared in the individual financial statement will not be taken into account by the *Agency*.

If an individual financial statement is not submitted for a reporting period, it may be included in the periodic financial report for the next reporting period.

The individual financial statements of the last reporting period must also detail the **receipts of the action** (see Article 5.3.3).

Each beneficiary must **certify** that:

- the information provided is full, reliable and true;
 - the costs declared are eligible (see Article 6);
 - the costs can be substantiated by adequate records and supporting documentation (see Article 18) that will be produced upon request (see Article 17) or in the context of checks, reviews, audits and investigations (see Article 22), and
 - for the last reporting period: that all the receipts have been declared (see Article 5.3.3);
- (ii) an **explanation of the use of resources** and the information on subcontracting (see Article 13) and in-kind contributions provided by third parties (see Articles 11 and 12) from each beneficiary, for the reporting period concerned;
- (iii) *not applicable*;
- (iv) a ‘**periodic summary financial statement**’ (see Annex 4), created automatically by the electronic exchange system, consolidating the individual financial statements for the reporting period concerned and including — except for the last reporting period — the **request for interim payment**.

20.4 Final report — Request for payment of the balance

In addition to the periodic report for the last reporting period, the coordinator must submit the final report within 60 days following the end of the last reporting period.

The **final report** must include the following:

- (a) a ‘**final technical report**’ with a **summary** for publication containing:
- (i) an overview of the results and their exploitation and dissemination;
 - (ii) the conclusions on the action, and
 - (iii) the socio-economic impact of the action;
- (b) a ‘**final financial report**’ containing:
- (i) a ‘**final summary financial statement**’ (see Annex 4), created automatically by the electronic exchange system, consolidating the individual financial statements for all reporting periods and including the **request for payment of the balance** and
 - (ii) a ‘**certificate on the financial statements**’ (drawn up in accordance with Annex 5) for each beneficiary, if it requests a total contribution of EUR 325 000 or more, as reimbursement of actual costs and unit costs calculated on the basis of its usual cost accounting practices (see Article 5.2 and Article 6.2, Point A).

20.5 Information on cumulative expenditure incurred

Not applicable

20.6 Currency for financial statements and conversion into euro

Financial statements must be drafted in euro.

Beneficiaries with accounting established in a currency other than the euro must convert the costs recorded in their accounts into euro, at the average of the daily exchange rates published in the C series of the *Official Journal of the European Union*, calculated over the corresponding reporting period.

If no daily euro exchange rate is published in the *Official Journal of the European Union* for the currency in question, they must be converted at the average of the monthly accounting rates published on the Commission's website, calculated over the corresponding reporting period.

Beneficiaries with accounting established in euro must convert costs incurred in another currency into euro according to their usual accounting practices.

20.7 Language of reports

All reports (technical and financial reports, including financial statements) must be submitted in the language of the Agreement.

20.8 Consequences of non-compliance — Suspension of the payment deadline — Termination

If the reports submitted do not comply with this Article, the *Agency* may suspend the payment deadline (see Article 47) and apply any of the other measures described in Chapter 6.

If the coordinator breaches its obligation to submit the reports and if it fails to comply with this obligation within 30 days following a written reminder sent by the *Agency*, the Agreement may be terminated (see Article 50).

ARTICLE 21 — PAYMENTS AND PAYMENT ARRANGEMENTS

21.1 Payments to be made

The following payments will be made to the coordinator:

- one **pre-financing payment**;
- one or more **interim payments**, on the basis of the request(s) for interim payment (see Article 20), and
- one **payment of the balance**, on the basis of the request for payment of the balance (see Article 20).

21.2 Pre-financing payment — Amount — Amount retained for the Guarantee Fund

The aim of the pre-financing is to provide the beneficiaries with a float.

It remains the property of the *EU* until the payment of the balance.

The amount of the pre-financing payment will be EUR [REDACTED]

The *Agency* will — except if Article 48 applies — make the pre-financing payment to the coordinator within 30 days either from the entry into force of the Agreement (see Article 58) or from 10 days before the starting date of the action (see Article 3), whichever is the latest.

An amount of EUR [REDACTED] corresponding to 5% of the maximum grant amount (see Article 5.1), is retained by the *Agency* from the pre-financing payment and transferred into the '**Guarantee Fund**'.

21.3 Interim payments — Amount — Calculation

Interim payments reimburse the eligible costs incurred for the implementation of the action during the corresponding reporting periods.

The *Agency* will pay to the coordinator the amount due as interim payment within 90 days from receiving the periodic report (see Article 20.3), except if Articles 47 or 48 apply.

Payment is subject to the approval of the periodic report. Its approval does not imply recognition of the compliance, authenticity, completeness or correctness of its content.

The **amount due as interim payment** is calculated by the *Agency* in the following steps:

Step 1 – Application of the reimbursement rates

Step 2 – Limit to 90% of the maximum grant amount

21.3.1 Step 1 — Application of the reimbursement rates

The reimbursement rate(s) (see Article 5.2) are applied to the eligible costs (actual costs, unit costs and flat-rate costs ; see Article 6) declared by the beneficiaries (see Article 20) and approved by the *Agency* (see above) for the concerned reporting period.

21.3.2 Step 2 — Limit to 90% of the maximum grant amount

The total amount of pre-financing and interim payments must not exceed 90% of the maximum grant amount set out in Article 5.1. The maximum amount for the interim payment will be calculated as follows:

{90% of the maximum grant amount (see Article 5.1)

minus

{pre-financing and previous interim payments}}.

21.4 Payment of the balance — Amount — Calculation — Release of the amount retained for the Guarantee Fund

The payment of the balance reimburses the remaining part of the eligible costs incurred by the beneficiaries for the implementation of the action.

If the total amount of earlier payments is greater than the final grant amount (see Article 5.3), the payment of the balance takes the form of a recovery (see Article 44).

If the total amount of earlier payments is lower than the final grant amount, the *Agency* will pay the balance within 90 days from receiving the final report (see Article 20.4), except if Articles 47 or 48 apply.

Payment is subject to the approval of the final report. Its approval does not imply recognition of the compliance, authenticity, completeness or correctness of its content.

The **amount due as the balance** is calculated by the *Agency* by deducting the total amount of pre-financing and interim payments (if any) already made, from the final grant amount determined in accordance with Article 5.3:

{final grant amount (see Article 5.3)

minus

{pre-financing and interim payments (if any) made} }.

At the payment of the balance, the amount retained for the Guarantee Fund (see above) will be released and:

- if the balance is positive: the amount released will be paid in full to the coordinator together with the amount due as the balance;
- if the balance is negative (payment of the balance taking the form of recovery): it will be deducted from the amount released (see Article 44.1.2). If the resulting amount:
 - is positive, it will be paid to the coordinator
 - is negative, it will be recovered.

The amount to be paid may however be offset — without the beneficiary's consent — against any other amount owed by the beneficiary to the *Agency*, the Commission or another executive agency (under the EU or Euratom budget), up to the maximum EU contribution indicated, for that beneficiary, in the estimated budget (see Annex 2).

21.5 Notification of amounts due

When making payments, the *Agency* will formally notify to the coordinator the amount due, specifying whether it concerns an interim payment or the payment of the balance.

For the payment of the balance, the notification will also specify the final grant amount.

In the case of reduction of the grant or recovery of undue amounts, the notification will be preceded by the contradictory procedure set out in Articles 43 and 44.

21.6 Currency for payments

The *Agency* will make all payments in euro.

21.7 Payments to the coordinator — Distribution to the beneficiaries

Payments will be made to the coordinator.

Payments to the coordinator will discharge the *Agency* from its payment obligation.

The coordinator must distribute the payments between the beneficiaries without unjustified delay.

Pre-financing may however be distributed only:

- (a) if the minimum number of beneficiaries set out in the call for proposals has acceded to the Agreement (see Article 56) and
- (b) to beneficiaries that have acceded to the Agreement (see Article 56).

21.8 Bank account for payments

All payments will be made to the following bank account:

Name of bank: [REDACTED]
Address of branch: [REDACTED]
Full name of the account holder: [REDACTED] SA
Full account number (including bank codes):
[REDACTED]

21.9 Costs of payment transfers

The cost of the payment transfers is borne as follows:

- the *Agency* bears the cost of transfers charged by its bank;
- the beneficiary bears the cost of transfers charged by its bank;
- the party causing a repetition of a transfer bears all costs of the repeated transfer.

21.10 Date of payment

Payments by the *Agency* are considered to have been carried out on the date when they are debited to its account.

21.11 Consequences of non-compliance

21.11.1 If the *Agency* does not pay within the payment deadlines (see above), the beneficiaries are entitled to **late-payment interest** at the rate applied by the European Central Bank (ECB) for its main refinancing operations in euros ('reference rate'), plus three and a half points. The reference rate is the rate in force on the first day of the month in which the payment deadline expires, as published in the C series of the *Official Journal of the European Union*.

If the late-payment interest is lower than or equal to EUR 200, it will be paid to the coordinator only upon request submitted within two months of receiving the late payment.

Late-payment interest is not due if all beneficiaries are EU Member States (including regional and local government authorities or other public bodies acting on behalf of a Member State for the purpose of this Agreement).

Suspension of the payment deadline or payments (see Articles 47 and 48) will not be considered as late payment.

Late-payment interest covers the period running from the day following the due date for payment (see above), up to and including the date of payment.

Late-payment interest is not considered for the purposes of calculating the final grant amount.

21.11.2 If the coordinator breaches any of its obligations under this Article, the grant may be reduced (see Article 43) and the Agreement or the participation of the coordinator may be terminated (see Article 50).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 22 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS

22.1 Checks, reviews and audits by the *Agency and the Commission*

22.1.1 Right to carry out checks

The *Agency or the Commission* will — during the implementation of the action or afterwards — check the proper implementation of the action and compliance with the obligations under the Agreement, including assessing deliverables and reports.

For this purpose the *Agency or the Commission* may be assisted by external persons or bodies.

The *Agency or the Commission* may also request additional information in accordance with Article 17. The *Agency or the Commission* may request beneficiaries to provide such information to it directly.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

22.1.2 Right to carry out reviews

The *Agency or the Commission* may — during the implementation of the action or afterwards — carry out reviews on the proper implementation of the action (including assessment of deliverables and reports), compliance with the obligations under the Agreement and continued scientific or technological relevance of the action.

Reviews may be started **up to two years after the payment of the balance**. They will be formally notified to the coordinator or beneficiary concerned and will be considered to have started on the date of the formal notification.

If the review is carried out on a third party (see Articles 10 to 16), the beneficiary concerned must inform the third party.

The *Agency or the Commission* may carry out reviews directly (using its own staff) or indirectly (using external persons or bodies appointed to do so). It will inform the coordinator or beneficiary concerned of the identity of the external persons or bodies. They have the right to object to the appointment on grounds of commercial confidentiality.

The coordinator or beneficiary concerned must provide — within the deadline requested — any information and data in addition to deliverables and reports already submitted (including information on the use of resources). The *Agency or the Commission* may request beneficiaries to provide such information to it directly.

The coordinator or beneficiary concerned may be requested to participate in meetings, including with external experts.

For **on-the-spot** reviews, the beneficiaries must allow access to their sites and premises, including to external persons or bodies, and must ensure that information requested is readily available.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

On the basis of the review findings, a '**review report**' will be drawn up.

The *Agency or the Commission* will formally notify the review report to the coordinator or beneficiary concerned, which has 30 days to formally notify observations ('**contradictory review procedure**').

Reviews (including review reports) are in the language of the Agreement.

22.1.3 Right to carry out audits

The *Agency or the Commission* may — during the implementation of the action or afterwards — carry out audits on the proper implementation of the action and compliance with the obligations under the Agreement.

Audits may be started **up to two years after the payment of the balance**. They will be formally notified to the coordinator or beneficiary concerned and will be considered to have started on the date of the formal notification.

If the audit is carried out on a third party (see Articles 10 to 16), the beneficiary concerned must inform the third party.

The *Agency or the Commission* may carry out audits directly (using its own staff) or indirectly (using external persons or bodies appointed to do so). It will inform the coordinator or beneficiary concerned of the identity of the external persons or bodies. They have the right to object to the appointment on grounds of commercial confidentiality.

The coordinator or beneficiary concerned must provide — within the deadline requested — any information (including complete accounts, individual salary statements or other personal data) to verify compliance with the Agreement. The *Agency or the Commission* may request beneficiaries to provide such information to it directly.

For **on-the-spot** audits, the beneficiaries must allow access to their sites and premises, including to external persons or bodies, and must ensure that information requested is readily available.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

On the basis of the audit findings, a **‘draft audit report’** will be drawn up.

The *Agency or the Commission* will formally notify the draft audit report to the coordinator or beneficiary concerned, which has 30 days to formally notify observations (**‘contradictory audit procedure’**). This period may be extended by the *Agency or the Commission* in justified cases.

The **‘final audit report’** will take into account observations by the coordinator or beneficiary concerned. The report will be formally notified to it.

Audits (including audit reports) are in the language of the Agreement.

The *Agency or the Commission* may also access the beneficiaries’ statutory records for the periodical assessment of unit costs or flat-rate amounts.

22.2 Investigations by the European Anti-Fraud Office (OLAF)

Under Regulations No 883/2013¹⁵ and No 2185/96¹⁶ (and in accordance with their provisions and procedures), the European Anti-Fraud Office (OLAF) may — at any moment during implementation of the action or afterwards — carry out investigations, including on-the-spot checks and inspections, to establish whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the EU.

22.3 Checks and audits by the European Court of Auditors (ECA)

Under Article 287 of the Treaty on the Functioning of the European Union (TFEU) and Article 161 of the Financial Regulation No 966/2012¹⁷, the European Court of Auditors (ECA) may — at any moment during implementation of the action or afterwards — carry out audits.

The ECA has the right of access for the purpose of checks and audits.

22.4 Checks, reviews, audits and investigations for international organisations

Not applicable

22.5 Consequences of findings in checks, reviews, audits and investigations — Extension of findings

22.5.1 Findings in this grant

¹⁵ Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.09.2013, p. 1).

¹⁶ Council Regulation (Euratom, EC) No 2185/1996 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities’ financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2).

¹⁷ Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1).

Findings in checks, reviews, audits or investigations carried out in the context of this grant may lead to the rejection of ineligible costs (see Article 42), reduction of the grant (see Article 43), recovery of undue amounts (see Article 44) or to any of the other measures described in Chapter 6.

Rejection of costs or reduction of the grant after the payment of the balance will lead to a revised final grant amount (see Article 5.4).

Findings in checks, reviews, audits or investigations may lead to a request for amendment for the modification of Annex 1 (see Article 55).

Checks, reviews, audits or investigations that find systemic or recurrent errors, irregularities, fraud or breach of obligations may also lead to consequences in other EU or Euratom grants awarded under similar conditions (**‘extension of findings from this grant to other grants’**).

Moreover, findings arising from an OLAF investigation may lead to criminal prosecution under national law.

22.5.2 Findings in other grants

The *Agency or the* Commission may extend findings from other grants to this grant (**‘extension of findings from other grants to this grant’**), if:

- (a) the beneficiary concerned is found, in other EU or Euratom grants awarded under similar conditions, to have committed systemic or recurrent errors, irregularities, fraud or breach of obligations that have a material impact on this grant and
- (b) those findings are formally notified to the beneficiary concerned — together with the list of grants affected by the findings — no later than two years after the payment of the balance of this grant.

The extension of findings may lead to the rejection of costs (see Article 42), reduction of the grant (see Article 43), recovery of undue amounts (see Article 44), suspension of payments (see Article 48), suspension of the action implementation (see Article 49) or termination (see Article 50).

22.5.3 Procedure

The *Agency or the* Commission will formally notify the beneficiary concerned the systemic or recurrent errors and its intention to extend these audit findings, together with the list of grants affected.

22.5.3.1 If the findings concern **eligibility of costs**: the formal notification will include:

- (a) an invitation to submit observations on the list of grants affected by the findings;
- (b) the request to submit **revised financial statements** for all grants affected;
- (c) the **correction rate for extrapolation** established by the *Agency or the* Commission on the basis of the systemic or recurrent errors, to calculate the amounts to be rejected if the beneficiary concerned:
 - (i) considers that the submission of revised financial statements is not possible or practicable or

(ii) does not submit revised financial statements.

The beneficiary concerned has 90 days from receiving notification to submit observations, revised financial statements or to propose a duly substantiated **alternative correction method**. This period may be extended by the *Agency or the Commission* in justified cases.

The amounts to be rejected will be determined on the basis of the revised financial statements, subject to their approval.

If the *Agency or the Commission* does not receive any observations or revised financial statements, does not accept the observations or the proposed alternative correction method or does not approve the revised financial statements, it will formally notify the beneficiary concerned the application of the initially notified correction rate for extrapolation.

If the *Agency or the Commission* accepts the alternative correction method proposed by the beneficiary concerned, it will formally notify the application of the accepted alternative correction method.

22.5.3.2 If the findings concern **improper implementation** or a **breach of another obligation**: the formal notification will include:

- (a) an invitation to submit observations on the list of grants affected by the findings and
- (b) the flat-rate the *Agency or the Commission* intends to apply according to the principle of proportionality.

The beneficiary concerned has 90 days from receiving notification to submit observations or to propose a duly substantiated alternative flat-rate.

If the *Agency or the Commission* does not receive any observations or does not accept the observations or the proposed alternative flat-rate, it will formally notify the beneficiary concerned the application of the initially notified flat-rate.

If the *Agency or the Commission* accepts the alternative flat-rate proposed by the beneficiary concerned, it will formally notify the application of the accepted alternative flat-rate.

22.6 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, any insufficiently substantiated costs will be ineligible (see Article 6) and will be rejected (see Article 42).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 23 — EVALUATION OF THE IMPACT OF THE ACTION

23.1 Right to evaluate the impact of the action

The *Agency or the Commission* may carry out interim and final evaluations of the impact of the action measured against the objective of the *EU* programme.

Evaluations may be started during implementation of the action and up to *five* years after the payment of the balance. The evaluation is considered to start on the date of the formal notification to the coordinator or beneficiaries.

The *Agency or the* Commission may make these evaluations directly (using its own staff) or indirectly (using external bodies or persons it has authorised to do so).

The coordinator or beneficiaries must provide any information relevant to evaluate the impact of the action, including information in electronic format.

23.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the *Agency* may apply the measures described in Chapter 6.

SECTION 3 RIGHTS AND OBLIGATIONS RELATED TO BACKGROUND AND RESULTS

SUBSECTION 1 GENERAL

ARTICLE 23a — MANAGEMENT OF INTELLECTUAL PROPERTY

23a.1 Obligation to take measures to implement the Commission Recommendation on the management of intellectual property in knowledge transfer activities

Beneficiaries that are universities or other public research organisations must take measures to implement the principles set out in Points 1 and 2 of the Code of Practice annexed to the Commission Recommendation on the management of intellectual property in knowledge transfer activities¹⁸.

This does not change the obligations set out in Subsections 2 and 3 of this Section.

The beneficiaries must ensure that researchers and third parties involved in the action are aware of them.

23a.2 Consequences of non-compliance

If a beneficiary breaches its obligations under this Article, the *Agency* may apply any of the measures described in Chapter 6.

SUBSECTION 2 RIGHTS AND OBLIGATIONS RELATED TO BACKGROUND

ARTICLE 24 — AGREEMENT ON BACKGROUND

24.1 Agreement on background

The beneficiaries must identify and agree (in writing) on the background for the action (**‘agreement on background’**).

¹⁸ Commission Recommendation C (2008) 1329 of 10.4.2008 on the management of intellectual property in knowledge transfer activities and the Code of Practice for universities and other public research institutions attached to this recommendation.

‘Background’ means any data, know-how or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that:

- (a) is held by the beneficiaries before they acceded to the Agreement, and
- (b) is needed to implement the action or exploit the results.

24.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 25 — ACCESS RIGHTS TO BACKGROUND

25.1 Exercise of access rights — Waiving of access rights — No sub-licensing

To exercise access rights, this must first be requested in writing (**‘request for access’**).

‘Access rights’ means rights to use results or background under the terms and conditions laid down in this Agreement.

Waivers of access rights are not valid unless in writing.

Unless agreed otherwise, access rights do not include the right to sub-license.

25.2 Access rights for other beneficiaries, for implementing their own tasks under the action

The beneficiaries must give each other access — on a royalty-free basis — to background needed to implement their own tasks under the action, unless the beneficiary that holds the background has — before acceding to the Agreement —:

- (a) informed the other beneficiaries that access to its background is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel), or
- (b) agreed with the other beneficiaries that access would not be on a royalty-free basis.

25.3 Access rights for other beneficiaries, for exploiting their own results

The beneficiaries must give each other access — under fair and reasonable conditions — to background needed for exploiting their own results, unless the beneficiary that holds the background has — before acceding to the Agreement — informed the other beneficiaries that access to its background is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel).

‘Fair and reasonable conditions’ means appropriate conditions, including possible financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged.

Requests for access may be made — unless agreed otherwise — up to one year after the period set out in Article 3.

25.4 Access rights for affiliated entities

Unless otherwise agreed in the consortium agreement, access to background must also be given — under fair and reasonable conditions (see above; Article 25.3) and unless it is subject to legal restrictions or limits, including those imposed by the rights of third parties (including personnel) — to affiliated entities¹⁹ established in an EU Member State or ‘associated country’²⁰, if this is needed to exploit the results generated by the beneficiaries to which they are affiliated.

Unless agreed otherwise (see above; Article 25.1), the affiliated entity concerned must make the request directly to the beneficiary that holds the background.

Requests for access may be made — unless agreed otherwise — up to one year after the period set out in Article 3.

25.5 Access rights for third parties

Not applicable

25.6 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

SUBSECTION 3 RIGHTS AND OBLIGATIONS RELATED TO RESULTS

ARTICLE 26 — OWNERSHIP OF RESULTS

26.1 Ownership by the beneficiary that generates the results

Results are owned by the beneficiary that generates them.

¹⁹ For the definition, see Article 2.1(2) of the Rules for Participation Regulation No 1290/2013: ‘**affiliated entity**’ means any legal entity that is under the direct or indirect control of a participant, or under the same direct or indirect control as the participant, or that is directly or indirectly controlling a participant.

‘Control’ may take any of the following forms:

- (a) the direct or indirect holding of more than 50% of the nominal value of the issued share capital in the legal entity concerned, or of a majority of the voting rights of the shareholders or associates of that entity;
- (b) the direct or indirect holding, in fact or in law, of decision-making powers in the legal entity concerned.

However the following relationships between legal entities shall not in themselves be deemed to constitute controlling relationships:

- (a) the same public investment corporation, institutional investor or venture-capital company has a direct or indirect holding of more than 50% of the nominal value of the issued share capital or a majority of voting rights of the shareholders or associates;
- (b) the legal entities concerned are owned or supervised by the same public body.

²⁰ For the definition, see Article 2.1(3) of the Rules for Participation Regulation No 1290/2013: ‘**associated country**’ means a third country which is party to an international agreement with the Union, as identified in *Article 7 of Horizon 2020 Framework Programme Regulation No 1291/2013*. *Article 7 sets out the conditions for association of non-EU countries to Horizon 2020*.

‘Results’ means any (tangible or intangible) output of the action such as data, knowledge or information — whatever its form or nature, whether it can be protected or not — that is generated in the action, as well as any rights attached to it, including intellectual property rights.

26.2 Joint ownership by several beneficiaries

Two or more beneficiaries own results jointly if:

- (a) they have jointly generated them and
- (b) it is not possible to:
 - (i) establish the respective contribution of each beneficiary, or
 - (ii) separate them for the purpose of applying for, obtaining or maintaining their protection (see Article 27).

The joint owners must agree (in writing) on the allocation and terms of exercise of their joint ownership (**‘joint ownership agreement’**), to ensure compliance with their obligations under this Agreement.

Unless otherwise agreed in the joint ownership agreement, each joint owner may grant non-exclusive licences to third parties to exploit jointly-owned results (without any right to sub-license), if the other joint owners are given:

- (a) at least 45 days advance notice and
- (b) fair and reasonable compensation.

Once the results have been generated, joint owners may agree (in writing) to apply another regime than joint ownership (such as, for instance, transfer to a single owner (see Article 30) with access rights for the others).

26.3 Rights of third parties (including personnel)

If third parties (including personnel) may claim rights to the results, the beneficiary concerned must ensure that it complies with its obligations under the Agreement.

If a third party generates results, the beneficiary concerned must obtain all necessary rights (transfer, licences or other) from the third party, in order to be able to respect its obligations as if those results were generated by the beneficiary itself.

If obtaining the rights is impossible, the beneficiary must refrain from using the third party to generate the results.

26.4 Agency ownership, to protect results

26.4.1 *The Agency* may — with the consent of the beneficiary concerned — assume ownership of results to protect them, if a beneficiary intends — up to four years after the period set out in Article 3 — to disseminate its results without protecting them, except in any of the following cases:

- (a) the lack of protection is because protecting the results is not possible, reasonable or justified (given the circumstances);

- (b) the lack of protection is because there is a lack of potential for commercial or industrial exploitation, or
- (c) the beneficiary intends to transfer the results to another beneficiary or third party established in an EU Member State or associated country, which will protect them.

Before the results are disseminated and unless any of the cases above under Points (a), (b) or (c) applies, the beneficiary must formally notify the *Agency* and at the same time inform it of any reasons for refusing consent. The beneficiary may refuse consent only if it can show that its legitimate interests would suffer significant harm.

If the *Agency* decides to assume ownership, it will formally notify the beneficiary concerned within 45 days of receiving notification.

No dissemination relating to these results may before the end of this period or, if the *Agency* takes a positive decision, until it has taken the necessary steps to protect the results.

26.4.2 *The Agency* may — with the consent of the beneficiary concerned — assume ownership of results to protect them, if a beneficiary intends — up to four years after the period set out in Article 3 — to stop protecting them or not to seek an extension of protection, except in any of the following cases:

- (a) the protection is stopped because of a lack of potential for commercial or industrial exploitation;
- (b) an extension would not be justified given the circumstances.

A beneficiary that intends to stop protecting results or not seek an extension must — unless any of the cases above under Points (a) or (b) applies — formally notify the *Agency* at least 60 days before the protection lapses or its extension is no longer possible and at the same time inform it of any reasons for refusing consent. The beneficiary may refuse consent only if it can show that its legitimate interests would suffer significant harm.

If the *Agency* decides to assume ownership, it will formally notify the beneficiary concerned within 45 days of receiving notification.

26.5 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to the any of the other measures described in Chapter 6.

ARTICLE 27 — PROTECTION OF RESULTS — VISIBILITY OF EU FUNDING

27.1 Obligation to protect the results

Each beneficiary must examine the possibility of protecting its results and must adequately protect them — for an appropriate period and with appropriate territorial coverage — if:

- (a) the results can reasonably be expected to be commercially or industrially exploited and
- (b) protecting them is possible, reasonable and justified (given the circumstances).

When deciding on protection, the beneficiary must consider its own legitimate interests and the legitimate interests (especially commercial) of the other beneficiaries.

27.2 Agency ownership, to protect the results

If a beneficiary intends not to protect its results, to stop protecting them or not seek an extension of protection, *the Agency* may — under certain conditions (see Article 26.4) — assume ownership to ensure their (continued) protection.

27.3 Information on EU funding

Applications for protection of results (including patent applications) filed by or on behalf of a beneficiary must — unless the *Agency* requests or agrees otherwise or unless it is impossible — include the following:

“The project leading to this application has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700626”.

27.4 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such a breach may also lead to any of the other measures described in Chapter 6.

ARTICLE 28 — EXPLOITATION OF RESULTS

28.1 Obligation to exploit the results

Each beneficiary must — up to four years after the period set out in Article 3 — take measures aiming to ensure ‘**exploitation**’ of its results (either directly or indirectly, in particular through transfer or licensing; see Article 30) by:

- (a) using them in further research activities (outside the action);
- (b) developing, creating or marketing a product or process;
- (c) creating and providing a service, or
- (d) using them in standardisation activities.

This does not change the security obligations in Article 37, which still apply.

28.2 Results that could contribute to European or international standards — Information on EU funding

If results are incorporated in a standard, the beneficiary concerned must — unless the *Agency* requests or agrees otherwise or unless it is impossible — ask the standardisation body to include the following statement in (information related to) the standard:

“Results incorporated in this standard received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700626”.

28.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced in accordance with Article 43.

Such a breach may also lead to any of the other measures described in Chapter 6.

ARTICLE 29 — DISSEMINATION OF RESULTS — OPEN ACCESS — VISIBILITY OF EU FUNDING

29.1 Obligation to disseminate results

Unless it goes against their legitimate interests, each beneficiary must — as soon as possible — ‘**disseminate**’ its results by disclosing them to the public by appropriate means (other than those resulting from protecting or exploiting the results), including in scientific publications (in any medium).

This does not change the obligation to protect results in Article 27, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply.

A beneficiary that intends to disseminate its results must give advance notice to the other beneficiaries of — unless agreed otherwise — at least 45 days, together with sufficient information on the results it will disseminate.

Any other beneficiary may object within — unless agreed otherwise — 30 days of receiving notification, if it can show that its legitimate interests in relation to the results or background would be significantly harmed. In such cases, the dissemination may not take place unless appropriate steps are taken to safeguard these legitimate interests.

If a beneficiary intends not to protect its results, it may — under certain conditions (see Article 26.4.1) — need to formally notify the *Agency* before dissemination takes place.

29.2 Open access to scientific publications

Each beneficiary must ensure open access (free of charge online access for any user) to all peer-reviewed scientific publications relating to its results.

In particular, it must:

- (a) as soon as possible and at the latest on publication, deposit a machine-readable electronic copy of the published version or final peer-reviewed manuscript accepted for publication in a repository for scientific publications;

Moreover, the beneficiary must aim to deposit at the same time the research data needed to validate the results presented in the deposited scientific publications.

- (b) ensure open access to the deposited publication — via the repository — at the latest:
 - (i) on publication, if an electronic version is available for free via the publisher, or

- (ii) within six months of publication (twelve months for publications in the social sciences and humanities) in any other case.
- (c) ensure open access — via the repository — to the bibliographic metadata that identify the deposited publication.

The bibliographic metadata must be in a standard format and must include all of the following:

- the terms “*European Union (EU)*” and “*Horizon 2020*”;
- the name of the action, acronym and grant number;
- the publication date, and length of embargo period if applicable, and
- a persistent identifier.

29.3 Open access to research data

Not applicable

29.4 Information on EU funding — Obligation and right to use the EU emblem

Unless the *Agency* requests or agrees otherwise or unless it is impossible, any dissemination of results (in any form, including electronic) must:

- (a) display the EU emblem and
- (b) include the following text:

“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700626”.

When displayed together with another logo, the EU emblem must have appropriate prominence.

For the purposes of their obligations under this Article, the beneficiaries may use the EU emblem without first obtaining approval from the *Agency*.

This does not however give them the right to exclusive use.

Moreover, they may not appropriate the EU emblem or any similar trademark or logo, either by registration or by any other means.

29.5 Disclaimer excluding *Agency* responsibility

Any dissemination of results must indicate that it reflects only the author's view and that the *Agency* is not responsible for any use that may be made of the information it contains.

29.6 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such a breach may also lead to any of the other measures described in Chapter 6.

ARTICLE 30 — TRANSFER AND LICENSING OF RESULTS

30.1 Transfer of ownership

Each beneficiary may transfer ownership of its results.

It must however ensure that its obligations under Articles 26.2, 26.4, 27, 28, 29, 30 and 31 also apply to the new owner and that this owner has the obligation to pass them on in any subsequent transfer.

This does not change the security obligations in Article 37, which still apply.

Unless agreed otherwise (in writing) for specifically-identified third parties or unless impossible under applicable EU and national laws on mergers and acquisitions, a beneficiary that intends to transfer ownership of results must give at least 45 days advance notice (or less if agreed in writing) to the other beneficiaries that still have (or still may request) access rights to the results. This notification must include sufficient information on the new owner to enable any beneficiary concerned to assess the effects on its access rights.

Unless agreed otherwise (in writing) for specifically-identified third parties, any other beneficiary may object within 30 days of receiving notification (or less if agreed in writing), if it can show that the transfer would adversely affect its access rights. In this case, the transfer may not take place until agreement has been reached between the beneficiaries concerned.

30.2 Granting licenses

Each beneficiary may grant licences to its results (or otherwise give the right to exploit them), if:

- (a) this does not impede the rights under Article 31 and
- (b) *not applicable*.

In addition to Points (a) and (b), exclusive licences for results may be granted only if all the other beneficiaries concerned have waived their access rights (see Article 31.1).

This does not change the dissemination obligations in Article 29 or security obligations in Article 37, which still apply.

30.3 Agency right to object to transfers or licensing

The Agency may — up to four years after the period set out in Article 3 — object to a transfer of ownership or the exclusive licensing of results, if:

- (a) it is to a third party established in a non-EU country not associated with Horizon 2020 and*
- (b) the Agency considers that the transfer or licence is not in line with EU interests regarding competitiveness or is inconsistent with ethical principles or security considerations.*

A beneficiary that intends to transfer ownership or grant an exclusive licence must formally notify the Agency before the intended transfer or licensing takes place and:

- *identify the specific results concerned;*
- *describe in detail the new owner or licensee and the planned or potential exploitation of the results, and*
- *include a reasoned assessment of the likely impact of the transfer or licence on EU competitiveness and its consistency with ethical principles and security considerations.*

The Agency may request additional information.

If the Agency decides to object to a transfer or exclusive licence, it must formally notify the beneficiary concerned within 60 days of receiving notification (or any additional information it has requested).

No transfer or licensing may take place in the following cases:

- *pending the Agency decision, within the period set out above;*
- *if the Agency objects;*
- *until the conditions are complied with, if the Agency objection comes with conditions.*

30.4 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such a breach may also lead to any of the other measures described in Chapter 6.

ARTICLE 31 — ACCESS RIGHTS TO RESULTS

31.1 Exercise of access rights — Waiving of access rights — No sub-licensing

The conditions set out in Article 25.1 apply.

The obligations set out in this Article do not change the security obligations in Article 37, which still apply.

31.2 Access rights for other beneficiaries, for implementing their own tasks under the action

The beneficiaries must give each other access — on a royalty-free basis — to results needed for implementing their own tasks under the action.

31.3 Access rights for other beneficiaries, for exploiting their own results

The beneficiaries must give each other — under fair and reasonable conditions (see Article 25.3) — access to results needed for exploiting their own results.

Requests for access may be made — unless agreed otherwise — up to one year after the period set out in Article 3.

31.4 Access rights of affiliated entities

Unless agreed otherwise in the consortium agreement, access to results must also be given — under fair and reasonable conditions (Article 25.3) — to affiliated entities established in an EU Member State or associated country, if this is needed for those entities to exploit the results generated by the beneficiaries to which they are affiliated.

Unless agreed otherwise (see above; Article 31.1), the affiliated entity concerned must make any such request directly to the beneficiary that owns the results.

Requests for access may be made — unless agreed otherwise — up to one year after the period set out in Article 3.

31.5 Access rights for the EU institutions, bodies, offices or agencies and EU Member States

The beneficiaries must give access to their results — on a royalty-free basis — to EU institutions, bodies, offices and agencies as well as EU Member States' national authorities, necessary for developing, implementing or monitoring their policies or programmes in this area.

Such access rights are limited to non-commercial and non-competitive use.

Access is conditional on an agreement to define specific conditions ensuring that:

- (a) the access will be used only for the intended purpose and*
- (b) appropriate confidentiality obligations are in place.*

The requesting EU Member State or EU institution, body, office or agency must inform all other EU Member States of such a request.

This does not change the security obligations in Article 37, which still apply.

31.6 Access rights for third parties

Not applicable

31.7 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

SECTION 4 OTHER RIGHTS AND OBLIGATIONS

ARTICLE 32 — RECRUITMENT AND WORKING CONDITIONS FOR RESEARCHERS

32.1 Obligation to take measures to implement the European Charter for Researchers and Code of Conduct for the Recruitment of Researchers

The beneficiaries must take all measures to implement the principles set out in the Commission Recommendation on the European Charter for Researchers and the Code of Conduct for the Recruitment of Researchers²², in particular regarding:

- working conditions;
- transparent recruitment processes based on merit, and
- career development.

The beneficiaries must ensure that researchers and third parties involved in the action are aware of them.

32.2 Consequences of non-compliance

If a beneficiary breaches its obligations under this Article, the *Agency* may apply any of the measures described in Chapter 6.

ARTICLE 33 — GENDER EQUALITY

33.1 Obligation to aim for gender equality

The beneficiaries must take all measures to promote equal opportunities between men and women in the implementation of the action. They must aim, to the extent possible, for a gender balance at all levels of personnel assigned to the action, including at supervisory and managerial level.

33.2 Consequences of non-compliance

If a beneficiary breaches its obligations under this Article, the *Agency* may apply any of the measures described in Chapter 6.

ARTICLE 34 — ETHICS

34.1 Obligation to comply with ethical principles

The beneficiaries must carry out the action in compliance with:

- (a) ethical principles (including the highest standards of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity²³ — and including, in particular, avoiding fabrication, falsification, plagiarism or other research misconduct) and

²² Commission Recommendation 2005/251/EC of 11 March 2005 on the European Charter for Researchers and on a Code of Conduct for the Recruitment of Researchers (OJ L 75, 22.3.2005, p. 67).

²³ The European Code of Conduct for Research Integrity of ALLEA (All European Academies) and ESF (European Science Foundation) of March 2011.

http://www.esf.org/fileadmin/Public_documents/Publications/Code_Conduct_ResearchIntegrity.pdf

(b) applicable international, EU and national law.

Funding will not be granted for activities carried out outside the EU if they are prohibited in all Member States.

The beneficiaries must ensure that the activities under the action have an exclusive focus on civil applications.

The beneficiaries must ensure that the activities under the action do not:

- (a) aim at human cloning for reproductive purposes;
- (b) intend to modify the genetic heritage of human beings which could make such changes heritable (with the exception of research relating to cancer treatment of the gonads, which may be financed), or
- (c) intend to create human embryos solely for the purpose of research or for the purpose of stem cell procurement, including by means of somatic cell nuclear transfer.

34.2 Activities raising ethical issues

Activities raising ethical issues must comply with the ‘**ethics requirements**’ set out in Annex 1.

Before the beginning of an activity raising an ethical issue, the coordinator must submit (see Article 52) to the *Agency* copy of:

- (a) any ethics committee opinion required under national law and
- (b) any notification or authorisation for activities raising ethical issues required under national law.

If these documents are not in English, the coordinator must also submit an English summary of the submitted opinions, notifications and authorisations (containing, if available, the conclusions of the committee or authority concerned).

If these documents are specifically requested for the action, the request must contain an explicit reference to the action title. The coordinator must submit a declaration by each beneficiary concerned that all the submitted documents cover the action tasks.

34.3 Activities involving human embryos or human embryonic stem cells

Activities involving research on human embryos or human embryonic stem cells may be carried out only if:

- they are set out in Annex 1 or
- the coordinator has obtained explicit approval (in writing) from the *Agency* (see Article 52).

34.4 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43) and the Agreement or participation of the beneficiary may be terminated (see Article 50).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 35 — CONFLICT OF INTERESTS

35.1 Obligation to avoid a conflict of interests

The beneficiaries must take all measures to prevent any situation where the impartial and objective implementation of the action is compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest (**‘conflict of interests’**).

They must formally notify to the *Agency* without delay any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation.

The *Agency* may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

35.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43) and the Agreement or participation of the beneficiary may be terminated (see Article 50).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 36 — CONFIDENTIALITY

36.1 General obligation to maintain confidentiality

During implementation of the action and for four years after the period set out in Article 3, the parties must keep confidential any data, documents or other material (in any form) that is identified as confidential at the time it is disclosed (**‘confidential information’**).

If a beneficiary requests, the *Agency* may agree to keep such information confidential for an additional period beyond the initial four years.

If information has been identified as confidential only orally, it will be considered to be confidential only if this is confirmed in writing within 15 days of the oral disclosure.

Unless otherwise agreed between the parties, they may use confidential information only to implement the Agreement.

The beneficiaries may disclose confidential information to their personnel or third parties involved in the action only if they:

- (a) need to know to implement the Agreement and
- (b) are bound by an obligation of confidentiality.

This does not change the security obligations in Article 37, which still apply.

The *Agency* may disclose confidential information to its staff, other EU institutions and bodies or third parties, if:

- (a) this is necessary to implement the Agreement or safeguard the EU's financial interests and
- (b) the recipients of the information are bound by an obligation of confidentiality.

Under the conditions set out in Article 4 of the Rules for Participation Regulation No 1290/2013²⁴, the Commission must moreover make available information on the results to other EU institutions, bodies, offices or agencies as well as Member States or associated countries.

The confidentiality obligations no longer apply if:

- (a) the disclosing party agrees to release the other party;
- (b) the information was already known by the recipient or is given to him without obligation of confidentiality by a third party that was not bound by any obligation of confidentiality;
- (c) the recipient proves that the information was developed without the use of confidential information;
- (d) the information becomes generally and publicly available, without breaching any confidentiality obligation, or
- (e) the disclosure of the information is required by EU or national law.

36.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 37 — SECURITY-RELATED OBLIGATIONS

37.1 Results with a security recommendation

‘Results with a security recommendation’ (see Annex I) may be disclosed or disseminated only under the conditions set out in Annex I.

Before disclosing such results to a third party (including linked third parties, such as affiliated entities), a beneficiary must inform the coordinator — which must request written approval from the Agency.

37.2 Classified results

Not applicable

37.3 Activities involving dual-use goods or dangerous materials and substances

Not applicable

37.4 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

²⁴ Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" (OJ L 347, 20.12.2013 p.81).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 38 — PROMOTING THE ACTION — VISIBILITY OF EU FUNDING

38.1 Communication activities by beneficiaries

38.1.1 Obligation to promote the action and its results

The beneficiaries must promote the action and its results, by providing targeted information to multiple audiences (including the media and the public) in a strategic and effective manner.

This does not change the dissemination obligations in Article 29, the confidentiality obligations in Article 36 or the security obligations in Article 37, all of which still apply.

Before engaging in a communication activity expected to have a major media impact, the beneficiaries must inform the *Agency* (see Article 52).

38.1.2 Information on EU funding — Obligation and right to use the EU emblem

Unless the *Agency* requests or agrees otherwise or unless it is impossible, any communication activity related to the action (including in electronic form, via social media, etc.) and any infrastructure, equipment and major results funded by the grant must:

- (a) display the EU emblem and
- (b) include the following text:

For communication activities: *“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700626”.*

For infrastructure, equipment and major results: *“This [infrastructure][equipment][insert type of result] is part of a project that has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700626”.*

When displayed together with another logo, the EU emblem must have appropriate prominence.

For the purposes of their obligations under this Article, the beneficiaries may use the EU emblem without first obtaining approval from the *Agency*.

This does not, however, give them the right to exclusive use.

Moreover, they may not appropriate the EU emblem or any similar trademark or logo, either by registration or by any other means.

38.1.3 Disclaimer excluding *Agency* responsibility

Any communication activity related to the action must indicate that it reflects only the author's view and that the *Agency* is not responsible for any use that may be made of the information it contains.

38.2 Communication activities by the *Agency*

38.2.1 Right to use beneficiaries’ materials, documents or information

The *Agency* may use, for its communication and publicising activities, information relating to the action, documents notably summaries for publication and public deliverables as well as any other material, such as pictures or audio-visual material that it receives from any beneficiary (including in electronic form).

This does not change the confidentiality obligations in Article 36 and the security obligations in Article 37, all of which still apply.

However, if the *Agency's* use of these materials, documents or information would risk compromising legitimate interests, the beneficiary concerned may request the *Agency* not to use it (see Article 52).

The right to use a beneficiary's materials, documents and information includes:

- (a) **use for its own purposes** (in particular, making them available to persons working for the *Agency* or any other EU institution, body, office or agency or body or institutions in EU Member States; and copying or reproducing them in whole or in part, in unlimited numbers);
- (b) **distribution to the public** (in particular, publication as hard copies and in electronic or digital format, publication on the internet, as a downloadable or non-downloadable file, broadcasting by any channel, public display or presentation, communicating through press information services, or inclusion in widely accessible databases or indexes);
- (c) **editing or redrafting** for communication and publicising activities (including shortening, summarising, inserting other elements (such as meta-data, legends, other graphic, visual, audio or text elements), extracting parts (e.g. audio or video files), dividing into parts, use in a compilation);
- (d) **translation**;
- (e) giving **access in response to individual requests** under Regulation No 1049/2001²⁵, without the right to reproduce or exploit;
- (f) **storage** in paper, electronic or other form;
- (g) **archiving**, in line with applicable document-management rules, and
- (h) the right to authorise **third parties** to act on its behalf or sub-license the modes of use set out in Points (b),(c),(d) and (f) to third parties if needed for the communication and publicising activities of the *Agency*.

If the right of use is subject to rights of a third party (including personnel of the beneficiary), the beneficiary must ensure that it complies with its obligations under this Agreement (in particular, by obtaining the necessary approval from the third parties concerned).

Where applicable (and if provided by the beneficiaries), the *Agency* will insert the following information:

“© – [year] – [name of the copyright owner]. All rights reserved. Licensed to the *Research Executive Agency (REA)* under conditions.”

²⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43.

38.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 43).

Such breaches may also lead to any of the other measures described in Chapter 6.

ARTICLE 39 — PROCESSING OF PERSONAL DATA

39.1 Processing of personal data by the *Agency and the Commission*

Any personal data under the Agreement will be processed by the *Agency or the Commission* under Regulation No 45/2001²⁶ and according to the ‘notifications of the processing operations’ to the Data Protection Officer (DPO) of the *Agency or the Commission* (publicly accessible in the DPO register).

Such data will be processed by the ‘**data controller**’ of the *Agency or the Commission* for the purposes of implementing, managing and monitoring the Agreement or protecting the financial interests of the EU or Euratom (including checks, reviews, audits and investigations; see Article 22).

The persons whose personal data are processed have the right to access and correct their own personal data. For this purpose, they must send any queries about the processing of their personal data to the data controller, via the contact point indicated in the ‘service specific privacy statement(s) (SSPS)’ that are published on the *Agency and the Commission* websites.

They also have the right to have recourse at any time to the European Data Protection Supervisor (EDPS).

39.2 Processing of personal data by the beneficiaries

The beneficiaries must process personal data under the Agreement in compliance with applicable EU and national law on data protection (including authorisations or notification requirements).

The beneficiaries may grant their personnel access only to data that is strictly necessary for implementing, managing and monitoring the Agreement.

The beneficiaries must inform the personnel whose personal data are collected and processed by the *Agency or the Commission*. For this purpose, they must provide them with the service specific privacy statement (SSPS) (see above), before transmitting their data to the *Agency or the Commission*.

39.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under Article 39.2, the *Agency* may apply any of the measures described in Chapter 6.

²⁶ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.01.2001, p. 1).

ARTICLE 40 — ASSIGNMENTS OF CLAIMS FOR PAYMENT AGAINST THE *AGENCY*

The beneficiaries may not assign any of their claims for payment against the *Agency* to any third party, except if approved by the *Agency* on the basis of a reasoned, written request by the coordinator (on behalf of the beneficiary concerned).

If the *Agency* has not accepted the assignment or the terms of it are not observed, the assignment will have no effect on it.

In no circumstances will an assignment release the beneficiaries from their obligations towards the *Agency*.

CHAPTER 5 DIVISION OF BENEFICIARIES' ROLES AND RESPONSIBILITIES

ARTICLE 41 — DIVISION OF BENEFICIARIES' ROLES AND RESPONSIBILITIES — RELATIONSHIP WITH COMPLEMENTARY BENEFICIARIES — RELATIONSHIP WITH PARTNERS OF A JOINT ACTION

41.1 Roles and responsibilities towards the *Agency*

The beneficiaries have full responsibility for implementing the action and complying with the Agreement.

The beneficiaries are jointly and severally liable for the **technical implementation** of the action as described in Annex 1. If a beneficiary fails to implement its part of the action, the other beneficiaries become responsible for implementing this part (without being entitled to any additional EU funding for doing so), unless the *Agency* expressly relieves them of this obligation.

The **financial responsibility** of each beneficiary is governed by Articles 44, 45 and 46.

41.2 Internal division of roles and responsibilities

The internal roles and responsibilities of the beneficiaries are divided as follows:

(a) Each **beneficiary** must:

- (i) keep information stored in the 'Beneficiary Register' (via the electronic exchange system) up to date (see Article 17);
- (ii) inform the coordinator immediately of any events or circumstances likely to affect significantly or delay the implementation of the action (see Article 17);
- (iii) submit to the coordinator in good time:
 - individual financial statements for itself and, if required, certificates on the financial statements (see Article 20);
 - the data needed to draw up the technical reports (see Article 20);

- ethics committee opinions and notifications or authorisations for activities raising ethical issues (see Article 34);
- any other documents or information required by the *Agency or the Commission* under the Agreement, unless the Agreement requires the beneficiary to submit this information directly to the *Agency or the Commission*.

(b) The **coordinator** must:

- (i) monitor that the action is implemented properly (see Article 7);
- (ii) act as the intermediary for all communications between the beneficiaries and the *Agency* (in particular, providing the *Agency* with the information described in Article 17), unless the Agreement specifies otherwise;
- (iii) request and review any documents or information required by the *Agency* and verify their completeness and correctness before passing them on to the *Agency*;
- (iv) submit the deliverables and reports to the *Agency* (see Articles 19 and 20);
- (v) ensure that all payments are made to the other beneficiaries without unjustified delay (see Article 21);
- (vi) inform the *Agency* of the amounts paid to each beneficiary, when required under the Agreement (see Articles 44 and 50) or requested by the *Agency*.

The coordinator may not delegate the above-mentioned tasks to any other beneficiary or subcontract them to any third party.

41.3 Internal arrangements between beneficiaries — Consortium agreement

The beneficiaries must have internal arrangements regarding their operation and co-ordination to ensure that the action is implemented properly. These internal arrangements must be set out in a written ‘consortium agreement’ between the beneficiaries, which may cover:

- *internal organisation of the consortium;*
- *management of access to the electronic exchange system;*
- *distribution of EU funding;*
- *additional rules on rights and obligations related to background and results (including whether access rights remain or not, if a beneficiary is in breach of its obligations) (see Section 3 of Chapter 4);*
- *settlement of internal disputes;*
- *liability, indemnification and confidentiality arrangements between the beneficiaries.*

The consortium agreement must not contain any provision contrary to the Agreement.

41.4 Relationship with complementary beneficiaries — Collaboration agreement*Not applicable***41.5 Relationship with partners of a joint action — Coordination agreement***Not applicable***CHAPTER 6 REJECTION OF COSTS — REDUCTION OF THE GRANT — RECOVERY — PENALTIES — DAMAGES — SUSPENSION — TERMINATION — FORCE MAJEURE****SECTION 1 REJECTION OF COSTS — REDUCTION OF THE GRANT — RECOVERY — PENALTIES****ARTICLE 42 — REJECTION OF INELIGIBLE COSTS****42.1 Conditions**

42.1.1 The *Agency* will — at the time of an **interim payment**, at the **payment of the balance** or **afterwards** — reject any costs which are ineligible (see Article 6), in particular following checks, reviews, audits or investigations (see Article 22).

42.1.2 The rejection may also be based on the **extension of findings from other grants to this grant**, under the conditions set out in Article 22.5.2.

42.2 Ineligible costs to be rejected — Calculation — Procedure

Ineligible costs will be rejected in full.

If the *Agency* rejects costs **without reduction of the grant** (see Article 43) or **recovery of undue amounts** (see Article 44), it will formally notify the coordinator or beneficiary concerned the rejection of costs, the amounts and the reasons why (if applicable, together with the notification of amounts due; see Article 21.5). The coordinator or beneficiary concerned may — within 30 days of receiving notification — formally notify the *Agency* of its disagreement and the reasons why.

If the *Agency* rejects costs **with reduction of the grant** or **recovery of undue amounts**, it will formally notify the rejection in the ‘**pre-information letter**’ on reduction or recovery set out in Articles 43 and 44.

42.3 Effects

If the *Agency* rejects costs at the time of an **interim payment** or the **payment of the balance**, it will deduct them from the total eligible costs declared, for the action, in the periodic or final summary financial statement (see Articles 20.3 and 20.4). It will then calculate the interim payment or payment of the balance as set out in Articles 21.3 or 21.4.

If the *Agency* — **after an interim payment but before the payment of the balance** — rejects costs declared in a periodic summary financial statement, it will deduct them from the total eligible costs declared, for the action, in the next periodic summary financial statement or in the final summary

financial statement. It will then calculate the interim payment or payment of the balance as set out in Articles 21.3 or 21.4.

If the *Agency* rejects costs **after the payment of the balance**, it will deduct the amount rejected from the total eligible costs declared, by the beneficiary, in the final summary financial statement. It will then calculate the revised final grant amount as set out in Article 5.4.

ARTICLE 43 — REDUCTION OF THE GRANT

43.1 Conditions

43.1.1 The *Agency* may — **at the payment of the balance or afterwards** — reduce the maximum grant amount (see Article 5.1), if the action has not been implemented properly as described in Annex 1 or another obligation under the Agreement has been breached.

43.1.2 The *Agency* may also reduce the maximum grant amount on the basis of the **extension of findings from other grants to this grant**, under the conditions set out in Article 22.5.2.

43.2 Amount to be reduced — Calculation — Procedure

The amount of the reduction will be proportionate to the improper implementation of the action or to the seriousness of the breach.

Before reduction of the grant, the *Agency* will formally notify a ‘**pre-information letter**’ to the coordinator or beneficiary concerned:

- informing it of its intention to reduce the grant, the amount it intends to reduce and the reasons why and
- inviting it to submit observations within 30 days of receiving notification

If the *Agency* does not receive any observations or decides to pursue reduction despite the observations it has received, it will formally notify **confirmation** of the reduction (if applicable, together with the notification of amounts due; see Article 21).

43.3 Effects

If the *Agency* reduces the grant at the time of **the payment of the balance**, it will calculate the reduced grant amount for the action and then determine the amount due as payment of the balance (see Articles 5.3.4 and 21.4).

If the *Agency* reduces the grant **after the payment of the balance**, it will calculate the revised final grant amount for the beneficiary concerned (see Article 5.4). If the revised final grant amount for the beneficiary concerned is lower than its share of the final grant amount, the *Agency* will recover the difference (see Article 44).

ARTICLE 44 — RECOVERY OF UNDUE AMOUNTS

44.1 Amount to be recovered — Calculation — Procedure

The *Agency* will — after **termination of the participation of a beneficiary, at the payment of the balance or afterwards** — claim back any amount that was paid but is not due under the Agreement.

Each beneficiary's financial responsibility in case of recovery is limited to its own debt, except for the amount retained for the Guarantee Fund (see Article 21.4).

44.1.1 Recovery after termination of a beneficiary's participation

If recovery takes place after termination of a beneficiary's participation (including the coordinator), the *Agency* will claim back the undue amount from the beneficiary concerned, by formally notifying it a debit note (see Article 50.2 and 50.3). This note will specify the amount to be recovered, the terms and the date for payment.

If payment is not made by the date specified in the debit note, the *Agency or the Commission* will **recover** the amount:

- (a) by '**offsetting**' it — without the beneficiary's consent — against any amounts owed to the beneficiary concerned by the *Agency*, the Commission or another executive agency (from the EU or Euratom budget).

In exceptional circumstances, to safeguard the EU's financial interests, the *Agency* may offset before the payment date specified in the debit note;

- (b) *not applicable*;

- (c) by **taking legal action** (see Article 57) or by **adopting an enforceable decision** under Article 299 of the Treaty on the Functioning of the EU (TFEU) and Article 79(2) of the Financial regulation No 966/2012.

If payment is not made by the date specified in the debit note, the amount to be recovered (see above) will be increased by **late-payment interest** at the rate set out in Article 21.11, from the day following the payment date in the debit note, up to and including the date the *Agency or the Commission* receives full payment of the amount.

Partial payments will be first credited against expenses, charges and late-payment interest and then against the principal.

Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2007/64/EC²⁷ applies.

44.1.2 Recovery at payment of the balance

If the payment of the balance takes the form of a recovery (see Article 21.4), the *Agency* will formally notify a '**pre-information letter**' to the coordinator:

- informing it of its intention to recover, the amount due as the balance and the reasons why;
- specifying that it intends to deduct the amount to be recovered from the amount retained for the Guarantee Fund;

²⁷ Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 05.12.2007, p. 1).

- requesting the coordinator to submit a report on the distribution of payments to the beneficiaries within 30 days of receiving notification, and
- inviting the coordinator to submit observations within 30 days of receiving notification.

If no observations are submitted or the *Agency* decides to pursue recovery despite the observations it has received, it will **confirm recovery** (together with the notification of amounts due; see Article 21.5) and:

- pay the difference between the amount to be recovered and the amount retained for the Guarantee Fund, **if the difference is positive** or
- formally notify to the coordinator a **debit note** for the difference between the amount to be recovered and the amount retained for the Guarantee Fund, **if the difference is negative**. This note will also specify the terms and the date for payment.

If the coordinator does not repay the *Agency* by the date in the debit note and has not submitted the report on the distribution of payments: the *Agency or the Commission* will **recover** the amount set out in the debit note from the coordinator (see below).

If the coordinator does not repay the *Agency* by the date in the debit note, but has submitted the report on the distribution of payments: the *Agency* will:

- (a) identify the beneficiaries for which the amount calculated as follows is negative:

$\{ \{ \{ \text{beneficiary's costs declared in the final summary financial statement and approved by the } \textit{Agency} \text{ multiplied by the reimbursement rate set out in Article 5.2 for the beneficiary concerned} \}$

divided by

the EU contribution for the action calculated according to Article 5.3.1 }

multiplied by

the final grant amount (see Article 5.3) },

minus

{pre-financing and interim payments received by the beneficiary} }.

- (b) formally notify to each beneficiary identified according to point (a) a **debit note** specifying the terms and date for payment. The amount of the debit note is calculated as follows:

{ {amount calculated according to point (a) for the beneficiary concerned

divided by

the sum of the amounts calculated according to point (a) for all the beneficiaries identified according to point (a) }

multiplied by

the amount set out in the debit note formally notified to the coordinator}.

If payment is not made by the date specified in the debit note, the *Agency* will **recover** the amount:

- (a) by '**offsetting**' it — without the beneficiary's consent — against any amounts owed to the beneficiary concerned by the *Agency*, the Commission or another executive agency (from the EU or Euratom budget).

In exceptional circumstances, to safeguard the EU's financial interests, the *Agency* may offset before the payment date specified in the debit note;

- (b) by **drawing on the Guarantee Fund**. The *Agency or the Commission* will formally notify the beneficiary concerned the debit note on behalf of the Guarantee Fund and recover the amount:

- (i) *not applicable*;

- (ii) by **taking legal action** (see Article 57) or by **adopting an enforceable decision** under Article 299 of the Treaty on the Functioning of the EU (TFEU) and Article 79(2) of the Financial Regulation No 966/2012.

If payment is not made by the date in the debit note, the amount to be recovered (see above) will be increased by **late-payment interest** at the rate set out in Article 21.11, from the day following the payment date in the debit note, up to and including the date the *Agency or the Commission* receives full payment of the amount.

Partial payments will be first credited against expenses, charges and late-payment interest and then against the principal.

Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2007/64/EC applies.

44.1.3 Recovery of amounts after payment of the balance

If, for a beneficiary, the revised final grant amount (see Article 5.4) is lower than its share of the final grant amount, it must repay the difference to the *Agency*.

The beneficiary's share of the final grant amount is calculated as follows:

$\left\{ \left\{ \text{beneficiary's costs declared in the final summary financial statement and approved by the } \textit{Agency} \right. \right.$
multiplied by the reimbursement rate set out in Article 5.2 for the beneficiary concerned}

divided by

the EU contribution for the action calculated according to Article 5.3.1 }

multiplied by

the final grant amount (see Article 5.3)}.

If the coordinator has not distributed amounts received (see Article 21.7), the *Agency* will also recover these amounts.

The *Agency* will formally notify a **pre-information letter** to the beneficiary concerned:

- informing it of its intention to recover, the due amount and the reasons why and
- inviting it to submit observations within 30 days of receiving notification.

If no observations are submitted or the *Agency* decides to pursue recovery despite the observations it has received, it will **confirm** the amount to be recovered and formally notify to the beneficiary concerned a **debit note**. This note will also specify the terms and the date for payment.

If payment is not made by the date specified in the debit note, the *Agency* will **recover** the amount:

- (a) by '**offsetting**' it — without the beneficiary's consent — against any amounts owed to the beneficiary concerned by the *Agency*, the Commission or another executive agency (from the EU or Euratom budget).

In exceptional circumstances, to safeguard the EU's financial interests, the *Agency* may offset before the payment date specified in the debit note;

- (b) by **drawing on the Guarantee Fund**. The *Agency or the Commission* will formally notify the beneficiary concerned the debit note on behalf of the Guarantee Fund and recover the amount:

(i) *not applicable*;

- (ii) by **taking legal action** (see Article 57) or by **adopting an enforceable decision** under Article 299 of the Treaty on the Functioning of the EU (TFEU) and Article 79(2) of the Financial Regulation No 966/2012.

If payment is not made by the date in the debit note, the amount to be recovered (see above) will be increased by **late-payment interest** at the rate set out in Article 21.11, from the day following the date for payment in the debit note, up to and including the date the *Agency or the Commission* receives full payment of the amount.

Partial payments will be first credited against expenses, charges and late-payment interest and then against the principal.

Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2007/64/EC applies.

ARTICLE 45 — ADMINISTRATIVE AND FINANCIAL PENALTIES

45.1 Conditions

Under Articles 109 and 131(4) of the Financial Regulation No 966/2012, the *Agency* may impose **administrative** and **financial penalties** if a beneficiary:

- (a) has committed substantial errors, irregularities or fraud or is in serious breach of its obligations under the Agreement or
- (b) has made false declarations about information required under the Agreement or for the submission of the proposal (or has not supplied such information).

Each beneficiary is responsible for paying the financial penalties imposed on it.

Under Article 109(3) of the Financial Regulation No 966/2012, the *Agency or the Commission* may — under certain conditions and limits — publish decisions imposing administrative or financial penalties.

45.2 Duration — Amount of penalty — Calculation

Administrative penalties exclude the beneficiary from all contracts and grants financed from the EU or Euratom budget for a maximum of five years from the date the infringement is established by the *Agency*.

If the beneficiary commits another infringement within five years of the date the first infringement is established, the *Agency* may extend the exclusion period up to 10 years.

Financial penalties will be between 2% and 10% of the maximum EU contribution indicated, for the beneficiary concerned, in the estimated budget (see Annex 2).

If the beneficiary commits another infringement within five years of the date the first infringement is established, the *Agency* may increase the rate of financial penalties to between 4% and 20%.

45.3 Procedure

Before applying a penalty, the *Agency* will formally notify the beneficiary concerned:

- informing it of its intention to impose a penalty, its duration or amount and the reasons why and
- inviting it to submit observations within 30 days.

If the *Agency* does not receive any observations or decides to impose the penalty despite of observations it has received, it will formally notify **confirmation** of the penalty to the beneficiary concerned and — in case of financial penalties — deduct the penalty from the payment of the balance or formally notify a **debit note**, specifying the amount to be recovered, the terms and the date for payment.

If payment is not made by the date specified in the debit note, the *Agency or the Commission* may **recover** the amount:

- (a) by '**offsetting**' it — without the beneficiary's consent — against any amounts owed to the beneficiary concerned by the *Agency, the Commission* or *another* executive agency (from the EU or Euratom budget).

In exceptional circumstances, to safeguard the EU's financial interests, the *Agency* may offset before the payment date specified in the debit note;

- (b) by **taking legal action** (see Article 57) or by **adopting an enforceable decision** under Article 299 of the Treaty on the Functioning of the EU (TFEU) and Article 79(2) of the Financial Regulation No 966/2012.

If payment is not made by the date in the debit note, the amount to be recovered (see above) will be increased by **late-payment interest** at the rate set out in Article 21.11, from the day following the payment date in the debit note, up to and including the date the *Agency or the Commission* receives full payment of the amount.

Partial payments will be first credited against expenses, charges and late-payment interest and then against the principal.

Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2007/64/EC applies.

SECTION 2 LIABILITY FOR DAMAGES

ARTICLE 46 — LIABILITY FOR DAMAGES

46.1 Liability of the *Agency*

The *Agency* cannot be held liable for any damage caused to the beneficiaries or to third parties as a consequence of implementing the Agreement, including for gross negligence.

The *Agency* cannot be held liable for any damage caused by any of the beneficiaries or third parties involved in the action, as a consequence of implementing the Agreement.

46.2 Liability of the beneficiaries

46.2.1 Conditions

Except in case of force majeure (see Article 51), the beneficiaries must compensate the *Agency* for any damage it sustains as a result of the implementation of the action or because the action was not implemented in full compliance with the Agreement.

Each beneficiary is responsible for paying the damages claimed from it.

46.2.2 Amount of damages - Calculation

The amount the *Agency* can claim from a beneficiary will correspond to the damage caused by that beneficiary.

46.2.3 Procedure

Before claiming damages, the *Agency* will formally notify the beneficiary concerned:

- informing it of its intention to claim damages, the amount and the reasons why and
- inviting it to submit observations within 30 days.

If the *Agency* does not receive any observations or decides to claim damages despite the observations it has received, it will formally notify **confirmation** of the claim for damages and a **debit note**, specifying the amount to be recovered, the terms and the date for payment.

If payment is not made by the date specified in the debit note, the *Agency or the Commission* may **recover** the amount:

- (a) by '**offsetting**' it — without the beneficiary's consent — against any amounts owed to the beneficiary concerned by the *Agency, the Commission* or *another* executive agency (from the EU or Euratom budget).

In exceptional circumstances, to safeguard the EU's financial interests, the *Agency* may offset before the payment date specified in the debit note;

- (b) by **taking legal action** (see Article 57) or by **adopting an enforceable decision** under Article 299 of the Treaty on the Functioning of the EU (TFEU) and Article 79(2) of the Financial Regulation No 966/2012.

If payment is not made by the date in the debit note, the amount to be recovered (see above) will be increased by **late-payment interest** at the rate set out in Article 21.11, from the day following the payment date in the debit note, up to and including the date the *Agency or the Commission* receives full payment of the amount.

Partial payments will be first credited against expenses, charges and late-payment interest and then against the principal.

Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2007/64/EC applies.

SECTION 3 SUSPENSION AND TERMINATION

ARTICLE 47 — SUSPENSION OF PAYMENT DEADLINE

47.1 Conditions

The *Agency* may — at any moment — suspend the payment deadline (see Article 21.2 to 21.4) if a request for payment (see Article 20) cannot be approved because:

- (a) it does not comply with the provisions of the Agreement (see Article 20);
- (b) the technical reports or financial reports have not been submitted or are not complete or additional information is needed, or
- (c) there is doubt about the eligibility of the costs declared in the financial statements and additional checks, reviews, audits or investigations are necessary.

47.2 Procedure

The *Agency* will formally notify the coordinator of the suspension and the reasons why.

The suspension will **take effect** the day notification is sent by the *Agency* (see Article 52).

If the conditions for suspending the payment deadline are no longer met, the suspension will be **lifted** — and the remaining period will resume.

If the suspension exceeds two months, the coordinator may request the *Agency* if the suspension will continue.

If the payment deadline has been suspended due to the non-compliance of the technical or financial reports (see Article 20) and the revised report or statement is not submitted or was submitted but is

also rejected, the *Agency* may also terminate the Agreement or the participation of the beneficiary (see Article 50.3.1(l)).

ARTICLE 48 — SUSPENSION OF PAYMENTS

48.1 Conditions

The *Agency* may — at any moment — suspend, in whole or in part, the pre-financing payment and interim payments for one or more beneficiaries or the payment of the balance for all beneficiaries, if a beneficiary:

- (a) has committed or is suspected of having committed substantial errors, irregularities, fraud or serious breach of obligations in the award procedure or under this Agreement or
- (b) has committed — in other EU or Euratom grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (**extension of findings from other grants to this grant**; see Article 22.5.2).

48.2 Procedure

Before suspending payments, the *Agency* will formally notify the coordinator:

- informing it of its intention to suspend payments and the reasons why and
- inviting it to submit observations within 30 days of receiving notification.

If the *Agency* does not receive observations or decides to pursue the procedure despite the observations it has received, it will formally notify **confirmation** of the suspension. Otherwise, it will formally notify that the suspension procedure is not continued.

The suspension will **take effect** the day the confirmation notification is sent by the *Agency*.

If the conditions for resuming payments are met, the suspension will be **lifted**. The *Agency* will formally notify the coordinator.

During the suspension, the periodic report(s) (see Article 20.3) must not contain any individual financial statements from the beneficiary concerned. When the *Agency* resumes payments, the coordinator may include them in the next periodic report.

The beneficiaries may suspend implementation of the action (see Article 49.1) or terminate the Agreement or the participation of the beneficiary concerned (see Article 50.1 and 50.2).

ARTICLE 49 — SUSPENSION OF THE ACTION IMPLEMENTATION

49.1 Suspension of the action implementation, by the beneficiaries

49.1.1 Conditions

The beneficiaries may suspend implementation of the action or any part of it, if exceptional circumstances — in particular *force majeure* (see Article 51) — make implementation impossible or excessively difficult.

49.1.2 Procedure

The coordinator must immediately formally notify to the *Agency* the suspension (see Article 52), stating:

- the reasons why and
- the expected date of resumption.

The suspension will **take effect** the day this notification is received by the *Agency*.

Once circumstances allow for implementation to resume, the coordinator must immediately formally notify the *Agency* and request an **amendment** of the Agreement to set the date on which the action will be resumed, extend the duration of the action and make other changes necessary to adapt the action to the new situation (see Article 55) — unless the Agreement or the participation of a beneficiary has been terminated (see Article 50).

The suspension will be **lifted** with effect from the resumption date set out in the amendment. This date may be before the date on which the amendment enters into force.

Costs incurred during suspension of the action implementation are not eligible (see Article 6).

49.2 Suspension of the action implementation, by the *Agency*

49.2.1 Conditions

The *Agency* may suspend implementation of the action or any part of it:

- (a) if a beneficiary has committed or is suspected of having committed substantial errors, irregularities, fraud or serious breach of obligations in the award procedure or under this Agreement;
- (b) if a beneficiary has committed — in other EU or Euratom grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (**extension of findings from other grants to this grant**; see Article 22.5.2), or
- (c) if the action is suspected of having lost its scientific or technological relevance.

49.2.2 Procedure

Before suspending implementation of the action, the *Agency* will formally notify the coordinator:

- informing it of its intention to suspend the implementation and the reasons why and
- inviting it to submit observations within 30 days of receiving notification.

If the *Agency* does not receive observations or decides to pursue the procedure despite the observations it has received, it will formally notify **confirmation** of the suspension. Otherwise, it will formally notify that the procedure is not continued.

The suspension will **take effect** five days after confirmation notification is received by the coordinator (or on a later date specified in the notification).

It will be **lifted** if the conditions for resuming implementation of the action are met.

The coordinator will be formally notified of the lifting and the Agreement will be **amended** to set the date on which the action will be resumed, extend the duration of the action and make other changes necessary to adapt the action to the new situation (see Article 55) — unless the Agreement has already been terminated (see Article 50).

The suspension will be lifted with effect from the resumption date set out in the amendment. This date may be before the date on which the amendment enters into force.

Costs incurred during suspension are not eligible (see Article 6).

The beneficiaries may not claim damages due to suspension by the *Agency* (see Article 46).

Suspension of the action implementation does not affect the *Agency's* right to terminate the Agreement or participation of a beneficiary (see Article 50), reduce the grant or recover amounts unduly paid (see Articles 43 and 44).

ARTICLE 50 — TERMINATION OF THE AGREEMENT OR OF THE PARTICIPATION OF ONE OR MORE BENEFICIARIES

50.1 Termination of the Agreement by the beneficiaries

50.1.1 Conditions and procedure

The beneficiaries may terminate the Agreement.

The coordinator must formally notify termination to the *Agency* (see Article 52), stating:

- the reasons why and
- the date the termination will take effect. This date must be after the notification.

If no reasons are given or if the *Agency* considers the reasons do not justify termination, the Agreement will be considered to have been '**terminated improperly**'.

The termination will **take effect** on the day specified in the notification.

50.1.2 Effects

The coordinator must — within 60 days from when termination takes effect — submit:

- (i) a periodic report (for the open reporting period until termination; see Article 20.3) and
- (ii) the final report (see Article 20.4).

If the *Agency* does not receive the reports within the deadline (see above), only costs which are included in an approved periodic report will be taken into account.

The *Agency* will **calculate** the final grant amount (see Article 5.3) and the balance (see Article 21.4) on the basis of the reports submitted. Only costs incurred until termination are eligible (see Article 6). Costs relating to contracts due for execution only after termination are not eligible.

Improper termination may lead to a reduction of the grant (see Article 43).

After termination, the beneficiaries' obligations (in particular Articles 20, 22, 23, Section 3 of Chapter 4, 36, 37, 38 and 40) continue to apply.

50.2 Termination of the participation of one or more beneficiaries, by the beneficiaries

50.2.1 Conditions and procedure

The participation of one or more beneficiaries may be terminated by the coordinator, on request of the beneficiary concerned or on behalf of the other beneficiaries.

The coordinator must formally notify termination to the *Agency* (see Article 52) and inform the beneficiary concerned.

If the coordinator's participation is terminated without its agreement, the formal notification must be done by another beneficiary (acting on behalf of the other beneficiaries).

The notification must include:

- the reasons why;
- the opinion of the beneficiary concerned (or proof that this opinion has been requested in writing);
- the date the termination takes effect. This date must be after the notification, and
- a request for amendment (see Article 55), with a proposal for reallocation of the tasks and the estimated budget of the beneficiary concerned (see Annexes 1 and 2) and, if necessary, the addition of one or more new beneficiaries (see Article 56). If termination takes effect after the period set out in Article 3, no request for amendment must be included unless the beneficiary concerned is the coordinator. In this case, the request for amendment must propose a new coordinator.

If this information is not given or if the *Agency* considers that the reasons do not justify termination, the participation will be considered to have been **terminated improperly**.

The termination will **take effect** on the day specified in the notification.

50.2.2 Effects

The coordinator must — within 30 days from when termination takes effect — submit:

- (i) a report on the distribution of payments to the beneficiary concerned and
- (ii) if termination takes effect during the period set out in Article 3, a '**termination report**' from the beneficiary concerned, for the open reporting period until termination, containing an overview of the progress of the work, an overview of the use of resources, the individual financial statement and, if applicable, the certificate on the financial statement (see Articles 20.3 and 20.4).

The information in the termination report must also be included in the periodic report for the next reporting period (see Article 20.3).

If the request for amendment is rejected by the *Agency*, (because it calls into question the decision awarding the grant or breaches the principle of equal treatment of applicants), the Agreement may be terminated according to Article 50.3.1(c).

If the request for amendment is accepted by the *Agency*, the Agreement is **amended** to introduce the necessary changes (see Article 55).

The *Agency* will **calculate** — on the basis of the periodic reports, the termination report and the report on the distribution of payments — if the (pre-financing and interim) payments received by the beneficiary concerned exceed the beneficiary's EU contribution (calculated by applying the reimbursement rate(s) to the eligible costs declared by the beneficiary and approved by the *Agency*). Only costs incurred by the beneficiary concerned until termination takes effect are eligible (see Article 6). Costs relating to contracts due for execution only after termination are not eligible.

- If the payments received **exceed the amounts due**:
 - if termination takes effect during the period set out in Article 3 and the request for amendment is accepted, the beneficiary concerned must repay to the coordinator the amount unduly received. The *Agency* will formally notify the amount unduly received and request the beneficiary concerned to repay it to the coordinator within 30 days of receiving notification. If it does not repay the coordinator, the *Agency* will draw upon the Guarantee Fund to pay the coordinator and then notify a **debit note** on behalf of the Guarantee Fund to the beneficiary concerned (see Article 44);
 - in all other cases (in particular if termination takes effect after the period set out in Article 3), the *Agency* will formally notify a **debit note** to the beneficiary concerned. If payment is not made by the date in the debit note, the Guarantee Fund will pay to the *Agency* the amount due and the *Agency* will notify a debit note on behalf of the Guarantee Fund to the beneficiary concerned (see Article 44);
 - if the beneficiary concerned is the former coordinator, it must repay the new coordinator according to the procedure above, unless:
 - termination is after an interim payment and
 - the former coordinator has not distributed amounts received as pre-financing or interim payments (see Article 21.7).

In this case, the *Agency* will formally notify a **debit note** to the former coordinator. If payment is not made by the date in the debit note, the Guarantee Fund will pay to the *Agency* the amount due. The *Agency* will then pay the new coordinator and notify a debit note on behalf of the Guarantee Fund to the former coordinator (see Article 44).

- If the payments received **do not exceed the amounts due**: amounts owed to the beneficiary concerned will be included in the next interim or final payment.

If the *Agency* does not receive the termination report within the deadline (see above), only costs included in an approved periodic report will be taken into account.

If the *Agency* does not receive the report on the distribution of payments within the deadline (see above), it will consider that:

- the coordinator did not distribute any payment to the beneficiary concerned and that
- the beneficiary concerned must not repay any amount to the coordinator.

Improper termination may lead to a reduction of the grant (see Article 43) or termination of the Agreement (see Article 50).

After termination, the concerned beneficiary's obligations (in particular Articles 20, 22, 23, Section 3 of Chapter 4, 36, 37, 38 and 40) continue to apply.

50.3 Termination of the Agreement or the participation of one or more beneficiaries, by the *Agency*

50.3.1 Conditions

The *Agency* may terminate the Agreement or the participation of one or more beneficiaries, if:

- (a) one or more beneficiaries do not accede to the Agreement (see Article 56);
- (b) a change to their legal, financial, technical, organisational or ownership situation is likely to substantially affect or delay the implementation of the action or calls into question the decision to award the grant;
- (c) following termination of participation for one or more beneficiaries (see above), the necessary changes to the Agreement would call into question the decision awarding the grant or breach the principle of equal treatment of applicants (see Article 55);
- (d) implementation of the action is prevented by force majeure (see Article 51) or suspended by the coordinator (see Article 49.1) and either:
 - (i) resumption is impossible, or
 - (ii) the necessary changes to the Agreement would call into question the decision awarding the grant or breach the principle of equal treatment of applicants;
- (e) a beneficiary is declared bankrupt, being wound up, having its affairs administered by the courts, has entered into an arrangement with creditors, has suspended business activities, or is subject to any other similar proceedings or procedures under national law;
- (f) a beneficiary (or a natural person who has the power to represent or take decisions on its behalf) has been found guilty of professional misconduct, proven by any means;
- (g) a beneficiary does not comply with the applicable national law on taxes and social security;
- (h) the action has lost scientific or technological relevance;
- (i) *not applicable*;
- (j) *not applicable*;

- (k) a beneficiary (or a natural person who has the power to represent or take decisions on its behalf) has committed fraud, corruption, or is involved in a criminal organisation, money laundering or any other illegal activity affecting the EU's financial interests;
- (l) a beneficiary (or a natural person who has the power to represent or take decisions on its behalf) has — in the award procedure or under the Agreement — committed:
 - (i) substantial errors, irregularities, fraud or
 - (ii) serious breach of obligations, including improper implementation of the action, submission of false information, failure to provide required information, breach of ethical principles;
- (m) a beneficiary has committed — in other EU or Euratom grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant ('**extension of findings from other grants to this grant**').

50.3.2 Procedure

Before terminating the Agreement or participation of one or more beneficiaries, the *Agency* will formally notify the coordinator:

- informing it of its intention to terminate and the reasons why and
- inviting it, within 30 days of receiving notification, to submit observations and — in case of Point (l.ii) above — to inform the *Agency* of the measures to ensure compliance with the obligations under the Agreement.

If the *Agency* does not receive observations or decides to pursue the procedure despite the observations it has received, it will formally notify to the coordinator **confirmation** of the termination and the date it will take effect. Otherwise, it will formally notify that the procedure is not continued.

The termination will **take effect**:

- for terminations under Points (b), (c), (e), (g), (h), (j), and (l.ii) above: on the day specified in the notification of the confirmation (see above);
- for terminations under Points (a), (d), (f), (i), (k), (l.i) and (m) above: on the day after the notification of the confirmation is received by the coordinator.

50.3.3 Effects

- (a) for **termination of the Agreement**:

The coordinator must — within 60 days from when termination takes effect — submit:

- (i) a periodic report (for the last open reporting period until termination; see Article 20.3) and
- (ii) a final report (see Article 20.4).

If the Agreement is terminated for breach of the obligation to submit the reports (see Articles 20.8 and 50.3.1(l)), the coordinator may not submit any reports after termination.

If the *Agency* does not receive the reports within the deadline (see above), only costs which are included in an approved periodic report will be taken into account.

The *Agency* will **calculate** the final grant amount (see Article 5.3) and the balance (see Article 21.4) on the basis of the reports submitted. Only costs incurred until termination takes effect are eligible (see Article 6). Costs relating to contracts due for execution only after termination are not eligible.

This does not affect the *Agency's* right to reduce the grant (see Article 43) or to impose administrative and financial penalties (Article 45).

The beneficiaries may not claim damages due to termination by the *Agency* (see Article 46).

After termination, the beneficiaries' obligations (in particular Articles 20, 22, 23, Section 3 of Chapter 4, 36, 37, 38 and 40) continue to apply.

(b) for termination of the participation of one or more beneficiaries:

The coordinator must — within 60 days from when termination takes effect — submit:

- (i) a report on the distribution of payments to the beneficiary concerned;
- (ii) a request for amendment (see Article 55), with a proposal for reallocation of the tasks and estimated budget of the beneficiary concerned (see Annexes 1 and 2) and, if necessary, the addition of one or more new beneficiaries (see Article 56). If termination is notified after the period set out in Article 3, no request for amendment must be submitted unless the beneficiary concerned is the coordinator. In this case the request for amendment must propose a new coordinator, and
- (iii) if termination takes effect during the period set out in Article 3, a **termination report** from the beneficiary concerned, for the open reporting period until termination, containing an overview of the progress of the work, an overview of the use of resources, the individual financial statement and, if applicable, the certificate on the financial statement (see Article 20).

The information in the termination report must also be included in the periodic report for the next reporting period (see Article 20.3).

If the request for amendment is rejected by the *Agency* (because it calls into question the decision awarding the grant or breaches the principle of equal treatment of applicants), the Agreement may be terminated according to Article 50.3.1(c).

If the request for amendment is accepted by the *Agency*, the Agreement is **amended** to introduce the necessary changes (see Article 55).

The *Agency* will **calculate** — on the basis of the periodic reports, the termination report and the report on the distribution of payments — if the (pre-financing and interim) payments received by the beneficiary concerned exceed the beneficiary's EU contribution (calculated by applying the reimbursement rate(s) to the eligible costs declared by the beneficiary and approved by the *Agency*). Only costs incurred by the beneficiary concerned until termination takes effect are eligible (see Article 6). Costs relating to contracts due for execution only after termination are not eligible.

- If the payments received **exceed the amounts due**:
 - if termination takes effect during the period set out in Article 3 and the request for amendment is accepted, the beneficiary concerned must repay to the coordinator the amount unduly received. The *Agency* will formally notify the amount unduly received and request the beneficiary concerned to repay it to the coordinator within 30 days of receiving notification. If it does not repay the coordinator, the *Agency* will draw upon the Guarantee Fund to pay the coordinator and then notify a debit note on behalf of the Guarantee Fund to the beneficiary concerned (see Article 44);
 - in all other cases, in particular if termination takes effect after the period set out in Article 3, the *Agency* will formally notify a **debit note** to the beneficiary concerned. If payment is not made by the date in the debit note, the Guarantee Fund will pay to the *Agency* the amount due and the *Agency* will notify a debit note on behalf of the Guarantee Fund to the beneficiary concerned (see Article 44);
 - if the beneficiary concerned is the former coordinator, it must repay the new coordinator the amount unduly received, unless:
 - termination takes effect after an interim payment and
 - the former coordinator has not distributed amounts received as pre-financing or interim payments (see Article 21.7)

In this case, the *Agency* will formally notify a **debit note** to the former coordinator. If payment is not made by the date in the debit note, the Guarantee Fund will pay to the *Agency* the amount due. The *Agency* will then pay the new coordinator and notify a debit note on behalf of the Guarantee Fund to the former coordinator (see Article 44).

- If the payments received **do not exceed the amounts due**: amounts owed to the beneficiary concerned will be included in the next interim or final payment.

If the *Agency* does not receive the termination report within the deadline (see above), only costs included in an approved periodic report will be taken into account.

If the *Agency* does not receive the report on the distribution of payments within the deadline (see above), it will consider that:

- the coordinator did not distribute any payment to the beneficiary concerned, and that

- the beneficiary concerned must not repay any amount to the coordinator.

After termination, the concerned beneficiary's obligations (in particular Articles 20, 22, 23, Section 3 of Chapter 4, 36, 37, 38 and 40) continue to apply.

SECTION 4 FORCE MAJEURE

ARTICLE 51 — FORCE MAJEURE

'Force majeure' means any situation or event that:

- prevents either party from fulfilling their obligations under the Agreement,
- was unforeseeable, exceptional situation and beyond the parties' control,
- was not due to error or negligence on their part (or on the part of third parties involved in the action), and
- proves to be inevitable in spite of exercising all due diligence.

The following cannot be invoked as force majeure:

- any default of a service, defect in equipment or material or delays in making them available, unless they stem directly from a relevant case of force majeure,
- labour disputes or strikes, or
- financial difficulties.

Any situation constituting force majeure must be formally notified to the other party without delay, stating the nature, likely duration and foreseeable effects.

The parties must immediately take all the necessary steps to limit any damage due to force majeure and do their best to resume implementation of the action as soon as possible.

The party prevented by force majeure from fulfilling its obligations under the Agreement cannot be considered in breach of them.

CHAPTER 7 FINAL PROVISIONS

ARTICLE 52 — COMMUNICATION BETWEEN THE PARTIES

52.1 Form and means of communication

Communication under the Agreement (information, requests, submissions, 'formal notifications', etc.) must:

- be made in writing and
- bear the number of the Agreement.

Until the payment of the balance: all communication must be made through the electronic exchange system and using the forms and templates provided there.

After the payment of the balance: formal notifications must be made by registered post with proof of delivery ('formal notification on paper').

Communications in the electronic exchange system must be made by persons authorised according to the 'Terms and Conditions of Use of the electronic exchange system'. For naming the authorised persons, each beneficiary must have designated — before the signature of this Agreement — a 'Legal Entity Appointed Representative (LEAR)'. The role and tasks of the LEAR are stipulated in his/her appointment letter (see Terms and Conditions of Use of the electronic exchange system).

If the electronic exchange system is temporarily unavailable, instructions will be given on the *Agency* and Commission websites.

52.2 Date of communication

Communications are considered to have been made when they are sent by the sending party (i.e. on the date and time they are sent through the electronic exchange system).

Formal notifications through the **electronic** exchange system are considered to have been made when they are received by the receiving party (i.e. on the date and time of acceptance by the receiving party, as indicated by the time stamp). A formal notification that has not been accepted within 10 days after sending is considered to have been accepted.

Formal notifications **on paper** sent by **registered post** with proof of delivery (only after the payment of the balance) are considered to have been made on either:

- the delivery date registered by the postal service or
- the deadline for collection at the post office.

If the electronic exchange system is temporarily unavailable, the sending party cannot be considered in breach of its obligation to send a communication within a specified deadline.

52.3 Addresses for communication

The **electronic** exchange system must be accessed via the following URL:

<https://ec.europa.eu/research/participants/portal/desktop/en/projects/>

The *Agency* will formally notify the coordinator and beneficiaries in advance any changes to this URL.

Formal notifications on paper (only after the payment of the balance) addressed **to the Agency** must be sent to the following address:

*Research Executive Agency (REA)
Safeguarding Secure Society
B-1049 Brussels Belgium*

Formal notifications on paper (only after the payment of the balance) addressed **to the beneficiaries** must be sent to their legal address as specified in the 'Beneficiary Register'.

ARTICLE 53 — INTERPRETATION OF THE AGREEMENT

53.1 Precedence of the Terms and Conditions over the Annexes

The provisions in the Terms and Conditions of the Agreement take precedence over its Annexes.

Annex 2 takes precedence over Annex 1.

53.2 Privileges and immunities

Not applicable

ARTICLE 54 — CALCULATION OF PERIODS, DATES AND DEADLINES

In accordance with Regulation No 1182/71²⁸, periods expressed in days, months or years are calculated from the moment the triggering event occurs.

The day during which that event occurs is not considered as falling within the period.

ARTICLE 55 — AMENDMENTS TO THE AGREEMENT

55.1 Conditions

The Agreement may be amended, unless the amendment entails changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

Amendments may be requested by any of the parties.

55.2 Procedure

The party requesting an amendment must submit a request for amendment signed in the electronic exchange system (see Article 52).

The coordinator submits and receives requests for amendment on behalf of the beneficiaries (see Annex 3).

If a change of coordinator is requested without its agreement, the submission must be done by another beneficiary (acting on behalf of the other beneficiaries).

The request for amendment must include:

- the reasons why;
- the appropriate supporting documents;
- for a change of coordinator without its agreement: the opinion of the coordinator (or proof that this opinion has been requested in writing).

²⁸ Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time-limits (OJ L 124, 8.6.1971, p. 1).

The *Agency* may request additional information.

If the party receiving the request agrees, it must sign the amendment in the electronic exchange system within 45 days of receiving notification (or any additional information the *Agency* has requested). If it does not agree, it must formally notify its disagreement within the same deadline. The deadline may be extended, if necessary for the assessment of the request. If no notification is received within the deadline, the request is considered to have been rejected.

An amendment **enters into force** on the day of the signature of the receiving party.

An amendment **takes effect** on the date agreed by the parties or, in the absence of such an agreement, on the date on which the amendment enters into force.

ARTICLE 56 — ACCESSION TO THE AGREEMENT

56.1 Accession of the beneficiaries mentioned in the Preamble

The other beneficiaries must accede to the Agreement by signing the Accession Form (see Annex 3) in the electronic exchange system (see Article 52) within 30 days after its entry into force (see Article 58).

They will assume the rights and obligations under the Agreement with effect from the date of its entry into force (see Article 58).

If a beneficiary does not accede to the Agreement within the above deadline, the coordinator must — within 30 days — request an amendment to make any changes necessary to ensure proper implementation of the action. This does not affect the *Agency's* right to terminate the Agreement (see Article 50).

56.2 Addition of new beneficiaries

In justified cases, the beneficiaries may request the addition of a new beneficiary.

For this purpose, the coordinator must submit a request for amendment in accordance with Article 55. It must include an Accession Form (see Annex 3) signed by the new beneficiary in the electronic exchange system (see Article 52).

New beneficiaries must assume the rights and obligations under the Agreement with effect from the date of their accession specified in the Accession Form (see Annex 3).

ARTICLE 57 — APPLICABLE LAW AND SETTLEMENT OF DISPUTES

57.1 Applicable law

The Agreement is governed by the applicable EU law, supplemented if necessary by the law of Belgium.

57.2 Dispute settlement

If a dispute concerning the interpretation, application or validity of the Agreement cannot be settled amicably, the General Court — or, on appeal, the Court of Justice of the European Union — has sole

jurisdiction. Such actions must be brought under Article 272 of the Treaty on the Functioning of the EU (TFEU).

If a dispute concerns administrative or financial penalties, offsetting or an enforceable decision under Article 299 TFEU (see Articles 44, 45 and 46), the beneficiaries must bring action before the General Court — or, on appeal, the Court of Justice of the European Union — under Article 263 TFEU. *Actions against enforceable decisions must be brought against the Commission (not against the Agency).*

ARTICLE 58 — ENTRY INTO FORCE OF THE AGREEMENT

The Agreement will enter into force on the day of signature by the *Agency* or the coordinator, depending on which is later.

SIGNATURES

For the coordinator

For the *Agency*





EUROPEAN COMMISSION
Research Executive Agency (REA)
Safeguarding Secure Society



ANNEX 1 (part A)

Research and Innovation action

NUMBER — 700626 — iCROSS

Table of Contents

1.1. The project summary.....	3
1.2. The list of beneficiaries.....	4
1.3. Workplan Tables - Detailed implementation.....	5
1.3.1. WT1 List of work packages.....	5
1.3.2. WT2 List of deliverables.....	6
1.3.3. WT3 Work package descriptions.....	11
Work package 1.....	11
Work package 2.....	13
Work package 3.....	17
Work package 4.....	21
Work package 5.....	24
Work package 6.....	28
Work package 7.....	31
Work package 8.....	35
1.3.4. WT4 List of milestones.....	38
1.3.5. WT5 Critical Implementation risks and mitigation actions.....	39
1.3.6 WT6 Summary of project effort in person-months.....	44
1.3.7. WT7 Tentative schedule of project reviews.....	45

1.1. The project summary

Project Number ¹	700626	Project Acronym ²	iCROSS
One form per project			
General information			
Project title ³	Intelligent Portable ContROl SyStem		
Starting date ⁴	01/09/2016		
Duration in months ⁵	36		
Call (part) identifier ⁶	H2020-BES-2015		
Topic	BES-05-2015 Border crossing points topic 1: Novel mobility concepts for land border security		
Fixed EC Keywords	Biometric equipment, Detection technology, Detection, identification and authentication		
Free keywords	Risk based approach, deception detection, anti-hacking cloud based architecture		
Abstract ⁷			
<p>iCROSS envisages to enable faster thorough border control for third country nationals crossing the borders of EU, with technologies that adopt the future development of the Schengen Border Management. The project will present an optimal mixture of an enhanced, voluntary form of a Registered Traveller Programme and an auxiliary solution for the Entry/Exit System based on involving bona fide travellers. iCROSS designs and implements a system that adopts mobility concepts and consists of a two-stage procedure, designed to reduce cost/time spent per traveller at the crossing station. It leverages software and hardware technologies ranging from portable readers/scanners, various emerging and novel subsystems for automatic controls, wireless networking for mobile controls, and secure backend storage and processing. The two-stage procedure includes: (A) the registration before the travel to gather initial personal, travel document and vehicle data, perform a short, automated, non-invasive interview with an avatar, subject to lie detection and link the traveller to any pre-existing authority data. Utilizing multifactor analytics and risk-based approach, the data registered is processed and correlated with publicly open data or external systems such as the SIS II. Processing will need the travellers consent as set in EU legislation and national law. (B) the actual control at the border that complements pre-registered information with results of security controls that are performed with a portable, wireless connected iCROSS unit that can be used inside buses/trains or any point. Multiple technologies check validity and authenticity of parameters (e.g. travel documents, visa, face recognition of traveller using passport picture, real-time automated non-invasive lie detection in interview by officer, etc.). The data collected are encrypted, securely transferred and analysed in real time, providing an automated decision support system for the border control officers.</p>			

1.2. List of Beneficiaries

Project Number ¹	700626	Project Acronym ²	iCROSS
-----------------------------	--------	------------------------------	--------

List of Beneficiaries

No	Name	Short name	Country	Project entry month ⁸	Project exit month
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	Luxembourg	1	36
2	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	ICCS	Greece	1	36
3	STREMBLE VENTURES LTD	STR	Cyprus	1	36
4	THE MANCHESTER METROPOLITAN UNIVERSITY	MMU	United Kingdom	1	36
5	ITTI SP ZOO	ITTI	Poland	1	36
6	EVERIS AEROESPACIAL Y DEFENSA SL	EVR	Spain	1	36
7	BIOSEC GROUP KORLATOLT FELELOSSEGU TARSASAG	BIO	Hungary	1	36
8	JAS TECHNOLOGIE SP ZOO	JAS	Poland	1	36
9	GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER	LUH	Germany	1	36
10	ORSZAGOS RENDOR - FOKAPITANYASAG	HNP	Hungary	1	36
11	KOMENDA GLOWNA STRAZY GRANICZNEJ	PBG	Poland	1	36
12	TRAILOSE METAFORES-METAFORIKES YPIRESIES EPIVATON KAI FORTIOU AE	TRA	Greece	1	36
13	LATVIAN STATE BORDER GUARD	BSG	Latvia	1	36

1.3. Workplan Tables - Detailed implementation

1.3.1. WT1 List of work packages

WP Number ⁹	WP Title	Lead beneficiary ¹⁰	Person-months ¹¹	Start month ¹²	End month ¹³
WP1	Ethics requirements	1 - ED		1	36
WP2	Relevant EU Legislation, Requirement Analyses and Reference Architecture	2 - ICCS		1	8
WP3	Technological Components and Subsystems Development	6 - EVR		3	24
WP4	Development of the iCROSS software platform and related interfaces	3 - STR		3	24
WP5	Integration and technical testing	1 - ED		15	30
WP6	Pilot Deployment and system evaluation	10 - HNP		15	36
WP7	Dissemination, Exploitation, Communication	5 - ITTI		1	36
WP8	Project Management and Quality Assurance	1 - ED		1	36
Total					

1.3.2. WT2 list of deliverables

Deliverable Number ¹⁴	Deliverable Title	WP number ⁹	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D1.1	GEN - Requirement No. 7	WP1	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	18
D1.2	OEI - Requirement No. 2	WP1	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	9
D1.3	GEN - Requirement No. 1	WP1	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	3
D1.4	GEN - Requirement No. 8	WP1	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	36
D2.1	Requirement Analysis Report	WP2	4 - MMU	Report	Confidential, only for members of the consortium (including the Commission Services)	4
D2.2	Reference Architecture and components specifications	WP2	2 - ICCS	Report	Confidential, only for members of the consortium (including the Commission Services)	8
D2.3	EU wide legal and ethical review report	WP2	9 - LUH	Report	Confidential, only for members of the consortium (including the Commission Services)	8
D3.1	Data Collection Devices - specifications	WP3	5 - ITTI	Report	Public	15
D3.2	First version of all technological tools and subsystems	WP3	6 - EVR	Report	Public	18

Deliverable Number ¹⁴	Deliverable Title	WP number ⁹	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
	(Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue)					
D3.3	Second version of all technological tools and subsystems for integration (Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue)	WP3	2 - ICCS	Report	Public	24
D4.1	First version of the iCROSS software platform	WP4	3 - STR	Report	Public	18
D4.2	Second version of the iCROSS software platform	WP4	1 - ED	Report	Public	24
D5.1	Integration plan	WP5	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	20
D5.2	Early version of the integrated prototype (limited functionality)	WP5	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	24
D5.3	Early version of the portable unit for border guards	WP5	8 - JAS	Report	Confidential, only for members of the consortium (including the Commission Services)	24
D5.4	Final version of the integrated prototype and portable unit (full functionality)	WP5	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	30
D5.5	Technical validation and evaluation report – User’s guide (involving education and training tools and material)	WP5	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	30
D5.6	Report on legal monitoring and	WP5	9 - LUH	Report	Confidential, only for members	30

Deliverable Number ¹⁴	Deliverable Title	WP number ⁹	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
	legal aspects implementation				of the consortium (including the Commission Services)	
D6.1	Experimental Design for Pilot Deployment and Evaluation	WP6	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	20
D6.2	Feedback of components evaluations with end users	WP6	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	22
D6.3	Analysis of pilot data feedback on early prototype	WP6	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	28
D6.4	Evaluation report of final prototype pilot deployment and Best Practices - Analysis of pilot feedback on final prototype	WP6	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	36
D7.1	Project Web Portal	WP7	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	3
D7.2	Project flyer	WP7	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	6
D7.3	Dissemination and communication plan	WP7	5 - ITTI	Report	Confidential, only for members of the consortium (including the Commission Services)	12
D7.4	Early Business Plan	WP7	1 - ED	Report	Confidential, only for members of the consortium (including the	12

Deliverable Number ¹⁴	Deliverable Title	WP number ⁹	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
					Commission Services)	
D7.5	Exploitation plan	WP7	6 - EVR	Report	Confidential, only for members of the consortium (including the Commission Services)	24
D7.6	Yearly communication report including communication material	WP7	5 - ITTI	Report	Public	24
D7.7	Project Flyer 2	WP7	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	20
D7.8	Dissemination and communication plan 2	WP7	5 - ITTI	Report	Confidential, only for members of the consortium (including the Commission Services)	24
D7.9	Dissemination and communication plan 3	WP7	5 - ITTI	Report	Confidential, only for members of the consortium (including the Commission Services)	36
D7.10	Exploitation plan 2	WP7	6 - EVR	Report	Confidential, only for members of the consortium (including the Commission Services)	36
D7.11	Yearly communication report including communication material 2	WP7	5 - ITTI	Report	Public	36
D8.1	Quality Management Plan	WP8	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	3
D8.2	Final Project Report	WP8	1 - ED	Report	Confidential, only for members of the consortium	36

Deliverable Number ¹⁴	Deliverable Title	WP number ⁹	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
					(including the Commission Services)	
D8.3	Periodic Progress Report	WP8	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	6
D8.4	Annual Report	WP8	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	12
D8.5	Periodic Progress Report 2	WP8	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	18
D8.6	Periodic Progress Report 3	WP8	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	30
D8.7	Annual Report 2	WP8	1 - ED	Report	Public	24

1.3.3. WT3 Work package descriptions

Work package number ⁹	WP1	Lead beneficiary ¹⁰	1 - ED
Work package title	Ethics requirements		
Start month	1	End month	36

Objectives

The objective is to ensure compliance with the 'ethics requirements' set out in this work package.

Description of work and role of partners

WP1 - Ethics requirements [Months: 1-36]

ED

This work package sets out the 'ethics requirements' that the project must comply with.

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D1.1	GEN - Requirement No. 7	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	18
D1.2	OEI - Requirement No. 2	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	9
D1.3	GEN - Requirement No. 1	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	3
D1.4	GEN - Requirement No. 8	1 - ED	Ethics	Confidential, only for members of the consortium (including the Commission Services)	36

Description of deliverables

The 'ethics requirements' that the project must comply with are included as deliverables in this work package.

D1.1 : GEN - Requirement No. 7 [18]

A report by the ethics Advisor must be submitted to the EU with the periodic reporting.

D1.2 : OEI - Requirement No. 2 [9]

The ethics of profiling and the risk of stigmatization of individuals and groups must be addressed in the context of WP2 and linked to the possibility of false positives. Furthermore, an appropriate mitigation plan must be included in D2.2 (Reference Architecture and Components Specifications).

D1.3 : GEN - Requirement No. 1 [3]

Given that the project involves complex and significant ethics issues, it is required that an independent Ethics Advisor (with appropriate expertise in data protection, surveillance and profiling) is appointed to oversee the implementation of the ethical concerns involved in this research.

D1.4 : GEN - Requirement No. 8 [36]

A report by the ethics Advisor must be submitted to the EU with the periodic reporting.

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
--------------------------------	-----------------	------------------	----------------------	-----------------------

Work package number ⁹	WP2	Lead beneficiary ¹⁰	2 - ICCS
Work package title	Relevant EU Legislation, Requirement Analyses and Reference Architecture		
Start month	1	End month	8

Objectives

- To analyse the end-user requirements and to assess user functional and technical needs.
- To identify the processes, technologies, challenges and their shortcomings through participatory research.
- To develop the iCROSS reference architecture and components / modules specifications.
- To conduct a thorough legislation review, both in EU and national level, to ensure iCROSS's legal compliance and to address privacy issues related to border control Pilot Cases i.e. agreements and informed consent.

Description of work and role of partners

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D2.1	Requirement Analysis Report	4 - MMU	Report	Confidential, only for members of the consortium (including the Commission Services)	4
D2.2	Reference Architecture and components specifications	2 - ICCS	Report	Confidential, only for members of the consortium (including the Commission Services)	8
D2.3	EU wide legal and ethical review report	9 - LUH	Report	Confidential, only for members of the consortium (including the Commission Services)	8

Description of deliverables

D2.1 Requirement Analysis Report (MMU) M4

D2.2 Reference Architecture and components specifications (EVR / ICCS) M8

D2.3 EU wide legal and ethical review report (LUH) M8

D2.1 : Requirement Analysis Report [4]

Report that includes: - a list of documented, actionable, measureable, testable, traceable requirements related to each stated project objective, to a level of detail sufficient for system design, - a set of scenarios to be used in the experimental design (Use Cases Scenarios based on the pilot cases) - identification and requirements of the pilot sites.

D2.2 : Reference Architecture and components specifications [8]

Specifications on the components' implementation, including system hardware, firmware and software, taking into account relevant standards. Besides the functional description, the non-functional requirements will be defined, such as real-time constraints (e.g. video and audio recording, image and face recognition, alerts, etc). In addition, aspects like capacity and performance will be investigated along with evolution qualities such as flexibility, extensibility and scalability.

D2.3 : EU wide legal and ethical review report [8]

A review of current legislation across the EU and legal and ethical issues arising from the deployment and use of the activity monitoring system will be identified, aligned with the use cases. Specific needs of the various stakeholders will be addressed in the project to assure that the planning and implementation of the overall solution is based on morally sound decisions.

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
MS1	Reference Architecture and components specifications	2 - ICCS	8	Completion of the reference architecture, and components

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
				technical and functional specifications

Work package number ⁹	WP3	Lead beneficiary ¹⁰	6 - EVR
Work package title	Technological Components and Subsystems Development		
Start month	3	End month	24

Objectives

<p>WP3 objectives aim to develop and technically test all the internal components and modules of the iCROSS system:</p> <ul style="list-style-type: none"> - To adopt the physical sensors and hardware to be used for data collection. - To develop the automated real time deception detection system (ADDS), the travel document authenticity analytics tool (DAAT), the face matching tool (FMT), the automated border control avatars - To provide hidden human and vehicle detection devices as alert tool - To design and implement the radio network to guarantee wireless connectivity and QoS

Description of work and role of partners

[illegible]

[illegible]

Partner number and short name	WP3 effort
1 - ED	
2 - ICCS	
3 - STR	
4 - MMU	
5 - ITTI	
6 - EVR	
7 - BIO	
8 - JAS	
9 - LUH	
10 - HNP	
12 - TRA	
Total	

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D3.1	Data Collection Devices - specifications	5 - ITTI	Report	Public	15
D3.2	First version of all technological tools and subsystems (Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue)	6 - EVR	Report	Public	18
D3.3	Second version of all technological tools and subsystems for integration (Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue)	2 - ICCS	Report	Public	24

Description of deliverables

D3.1 Data Collection Devices - specifications (ITTI) M15
D3.2 First version of all technological tools and subsystems (Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue) (EVR) M18
D3.3 Second version of all technological tools and subsystems for integration (Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue) (ICCS) M24

D3.1 : Data Collection Devices - specifications [15]

Identification of the necessary hardware sensors – cameras, scanners and other devices that will be used to capture all the necessary input. In-depth analysis of biometric sensors. State-of-the-art surveillance and document authentication instruments. SWOT analysis. Portable travel document scanners and related sensors. Selection of proper document RFID chip reader, QR code scanner, and UV for document authentication purposes.

D3.2 : First version of all technological tools and subsystems (Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue) [18]

Report about a first version of all technological tools and subsystems, including the Deception Detection System, biometrics, Document Authenticity Tool, Human and Vehicle Detection Tool, Avatar Based Dialogue and Portable Radar

D3.3 : Second version of all technological tools and subsystems for integration (Portable unit, ADDS, DAAT, portable radar, FMT, Avatar based dialogue) [24]

Report about the second version of all technological tools and subsystems, including the Deception Detection System, biometrics, Document Authenticity Tool, Human and Vehicle Detection Tool, Avatar Based Dialogue and Portable Radar

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
MS2	First version of all tools	6 - EVR	18	Completion of the first version of all system tools

Work package number ⁹	WP4	Lead beneficiary ¹⁰	3 - STR
Work package title	Development of the iCROSS software platform and related interfaces		
Start month	3	End month	24

Objectives

WP4 aims at the development of the iCROSS software tools and the relevant interfaces. Specifically to develop:

- the storage and retrieval infrastructure of the data collected.
- the risk based Assessment tool (RBAT) and the integrated automated border control analytics tool
- the social interface and interfaces with external and legacy systems
- the central data repository to collect the data into a single environment and the user interfaces for the agent

- WP4 aims at the development of the iCROSS software tools and the relevant interfaces. Specifically to develop:
- the storage and retrieval infrastructure of the data collected.
 - the risk based Assessment tool (RBAT) and the integrated automated border control analytics tool
 - the social interface and interfaces with external and legacy systems
 - the central data repository to collect the data into a single environment and the user interfaces for the agent

Description of work and role of partners

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Participation per Partner

Partner number and short name	WP4 effort
1 - ED	
2 - ICCS	
3 - STR	
5 - ITTI	
6 - EVR	
7 - BIO	
8 - JAS	
9 - LUH	
10 - HNP	
11 - PBG	
13 - BSG	
Total	

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D4.1	First version of the iCROSS software platform	3 - STR	Report	Public	18
D4.2	Second version of the iCROSS software platform	1 - ED	Report	Public	24

Description of deliverables

D4.1 First version of the iCROSS software platform (STR) M18
D4.2 Second version of the iCROSS software platform (ED) M24

D4.1 : First version of the iCROSS software platform [18]

Report on the first implementation of iCROSS solution, including first versions of Secure Cloud Based Storage, Processing and Data Protection, Risk Based Assessment Tool, external, legacy and social interfaces capabilities, mobile application, BCAT and AUI

D4.2 : Second version of the iCROSS software platform [24]

Report on the second implementation of iCROSS solution, including Secure Cloud Based Storage, Processing and Data Protection, Risk Based Assessment Tool, external, legacy and social interfaces capabilities, mobile application, BCAT and AUI

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
MS2	First version of all tools	6 - EVR	18	Completion of the first version of all system tools

Work package number ⁹	WP5	Lead beneficiary ¹⁰	1 - ED
Work package title	Integration and technical testing		
Start month	15	End month	30

Objectives

This WP deals with the integration of all components and technologies developed in WP3 and WP4 and their merging to complete functional prototypes that will undergo the verification and validation procedures with real end users in the following WP6. The overall final prototype will be defined by its hardware platform, developed components and integrated external devices (scanners and readers).

Description of work and role of partners

[illegible]



Participation per Partner

Partner number and short name	WP5 effort
1 - ED	
2 - ICCS	
3 - STR	
4 - MMU	
5 - ITTI	
6 - EVR	
7 - BIO	
8 - JAS	
9 - LUH	
12 - TRA	
Total	

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D5.1	Integration plan	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	20
D5.2	Early version of the integrated prototype (limited functionality)	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	24
D5.3	Early version of the portable unit for border guards	8 - JAS	Report	Confidential, only for members of the consortium (including the Commission Services)	24
D5.4	Final version of the integrated prototype and	1 - ED	Report	Confidential, only for members of the consortium (including the	30

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
	portable unit (full functionality)			Commission Services)	
D5.5	Technical validation and evaluation report – User's guide (involving education and training tools and material)	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	30
D5.6	Report on legal monitoring and legal aspects implementation	9 - LUH	Report	Confidential, only for members of the consortium (including the Commission Services)	30

Description of deliverables

D5.1 Integration plan (ED) M20

D5.2 Early version of the integrated prototype (limited functionality) (ED) M24

D5.3 Early version of the portable unit for border guards (JAS) M24

D5.4 Final version of the integrated prototype and portable unit (full functionality) (ED) M30

D5.5 Technical validation and evaluation report – User's guide (involving education and training tools and material) (ED) M30

D5.6 Report on legal monitoring and legal aspects implementation (LUH) M30

D5.1 : Integration plan [20]

Specification of a detailed roadmap for a continuous integration of the developed components and platforms, describing the integration process and responsibilities of the partners and setting the objectives of each integrated prototype. Registry of the dependencies between the components and a schedule of integration milestones with expected maturity for each component. Contingency plan.

D5.2 : Early version of the integrated prototype (limited functionality) [24]

Report on early prototype implementation of the integrated solution including limited functionality.

D5.3 : Early version of the portable unit for border guards [24]

Report on early prototype implementation of the portable unit for guards including limited functionality.

D5.4 : Final version of the integrated prototype and portable unit (full functionality) [30]

Report on the fully functional integrated prototype and portable unit for guards.

D5.5 : Technical validation and evaluation report – User's guide (involving education and training tools and material) [30]

- Description of the integration test cases with reference to their source code; - Log of execution of the integration test cases; - Register of raised issues with their status; - A user guide of the iCROSS system's overall implementation

D5.6 : Report on legal monitoring and legal aspects implementation [30]

Report on the monitoring of the technical and organisational developments and several version of the prototypes in order to evaluate them, in particular on their data protection implications throughout the project.

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
MS3	Early version of the integrated prototype (limited functionality)	1 - ED	24	Completion of the early integration and development of the early integrated prototype with limited functionality
MS4	Final version of the integrated prototype and portable unit (full functionality)	1 - ED	30	Completion of the final integrated prototype and portable unit with full functionality

Work package number ⁹	WP6	Lead beneficiary ¹⁰	10 - HNP
Work package title	Pilot Deployment and system evaluation		
Start month	15	End month	36

Objectives

The objectives of this work package are:

- To stepwise deploy the entire iCROSS system in the pilot sites of the end-users for pilot usage and evaluation
- To gather the end-user feedback on the pilot use of the overall framework
- To derive lessons learned and best practices of the comparative analyses and end user validation

Description of work and role of partners

[REDACTED]

[REDACTED]

--

Participation per Partner	
Partner number and short name	WP6 effort
1 - ED	
2 - ICCS	
3 - STR	
4 - MMU	
5 - ITTI	
6 - EVR	
7 - BIO	
8 - JAS	
9 - LUH	
10 - HNP	
11 - PBG	
12 - TRA	
13 - BSG	
Total	

List of deliverables					
Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D6.1	Experimental Design for Pilot Deployment and Evaluation	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	20
D6.2	Feedback of components evaluations with end users	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	22
D6.3	Analysis of pilot data feedback on early prototype	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	28

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D6.4	Evaluation report of final prototype pilot deployment and Best Practices - Analysis of pilot feedback on final prototype	10 - HNP	Report	Confidential, only for members of the consortium (including the Commission Services)	36

Description of deliverables

D6.1 Experimental Design for Pilot Deployment and Evaluation (HNP) M20
D6.2 Feedback of components evaluations with end users (HNP) M22
D6.3 Analysis of pilot data feedback on early prototype (HNP) M28
D6.4 Evaluation report of final prototype pilot deployment and Best Practices - Analysis of pilot feedback on final prototype (HNP) M36

D6.1 : Experimental Design for Pilot Deployment and Evaluation [20]

Report about a specific methodology for executing the experimental evaluation in order to capture the end-user feedback in a unified and consistent manner in all deployment sites.

D6.2 : Feedback of components evaluations with end users [22]

Report of an experimental evaluation that will capture the end-user feedback in a unified and consistent manner in all deployment sites.

D6.3 : Analysis of pilot data feedback on early prototype [28]

Collection and analysis of the evaluation of the components and collection of the feedback on the deployed prototypes in all pilots. Performance, cost and time calculation.

D6.4 : Evaluation report of final prototype pilot deployment and Best Practices - Analysis of pilot feedback on final prototype [36]

Final Evaluation Report that will include the results of each hypothesis tested, conclusions reached, and a thorough discussion on lessons learned.

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
MS5	Evaluation report of final prototype pilot deployment and Best Practices	10 - HNP	36	Completion of evaluation report for the final prototype pilot deployment and best practices

Work package number ⁹	WP7	Lead beneficiary ¹⁰	5 - ITTI
Work package title	Dissemination, Exploitation, Communication		
Start month	1	End month	36

Objectives

The objectives of this WP are: to develop the project communication infrastructure and material, to guarantee the impact on European economy through the planning and management of exploitation and dissemination and follow-on activities, to safeguard the process of exploitation of results and to investigate the market exploitation potentials. Furthermore, to ensure wide communication of the projects' results to all potential interested parties and the widest audience during the project lifecycle.

Description of work and role of partners

Participation per Partner

Partner number and short name	WP7 effort
1 - ED	
2 - ICCS	
3 - STR	
4 - MMU	

Partner number and short name	WP7 effort
5 - ITTI	
6 - EVR	
7 - BIO	
8 - JAS	
9 - LUH	
10 - HNP	
11 - PBG	
12 - TRA	
13 - BSG	
Total	

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D7.1	Project Web Portal	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	3
D7.2	Project flyer	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	6
D7.3	Dissemination and communication plan	5 - ITTI	Report	Confidential, only for members of the consortium (including the Commission Services)	12
D7.4	Early Business Plan	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	12
D7.5	Exploitation plan	6 - EVR	Report	Confidential, only for members of the consortium (including the Commission Services)	24

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D7.6	Yearly communication report including communication material	5 - ITTI	Report	Public	24
D7.7	Project Flyer 2	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	20
D7.8	Dissemination and communication plan 2	5 - ITTI	Report	Confidential, only for members of the consortium (including the Commission Services)	24
D7.9	Dissemination and communication plan 3	5 - ITTI	Report	Confidential, only for members of the consortium (including the Commission Services)	36
D7.10	Exploitation plan 2	6 - EVR	Report	Confidential, only for members of the consortium (including the Commission Services)	36
D7.11	Yearly communication report including communication material 2	5 - ITTI	Report	Public	36

Description of deliverables

D7.1 Project Web Portal (ED) M3
 D7.2 Project flyer (ED) M6, 20
 D7.3 Dissemination and communication plan (iTTI) M12,24,36
 D7.4 Early Business Plan (ED) M12
 D7.5 Exploitation plan (EVR) M24, 36
 D7.6 Yearly communication report including communication material (iTTI) M24,36
 D7.1 : Project Web Portal [3]
 Web portal of the project for dissemination, communication and awareness raising.
 D7.2 : Project flyer [6]
 Flyer of the project for dissemination, communication and awareness raising.
 D7.3 : Dissemination and communication plan [12]
 Communication planning and development of project materials

D7.4 : Early Business Plan [12] Early business plan of the project
D7.5 : Exploitation plan [24] Report of the potential exploitation paths for the project's results.
D7.6 : Yearly communication report including communication material [24] Yearly report of the communication plan and material.
D7.7 : Project Flyer 2 [20] Flyer of the project for dissemination, communication and awareness raising.
D7.8 : Dissemination and communication plan 2 [24] Communication planning and development of project materials
D7.9 : Dissemination and communication plan 3 [36] Communication planning and development of project materials
D7.10 : Exploitation plan 2 [36] Report of the potential exploitation paths for the project's results.
D7.11 : Yearly communication report including communication material 2 [36] Yearly report of the communication plan and material.

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
MS6	Exploitation plan	6 - EVR	36	Completion of the exploitation plan

Work package number ⁹	WP8	Lead beneficiary ¹⁰	1 - ED
Work package title	Project Management and Quality Assurance		
Start month	1	End month	36

Objectives

- To effectively monitor the project, in administrative, technical and financial terms, to ensure its strategic and everyday management and to offer the necessary interface to the EU services and external actors.
- To guarantee the adherence of the work to the overall project plans, available resources and timing.
- To ensure the high quality of iCROSS outcomes assuring that the project development will be in line with existing and emerging application guidelines and enabling the smooth execution and evaluation of activities
- To identify project risks by performing an effective risk management and risk mitigation actions.

Description of work and role of partners

--

Participation per Partner

Partner number and short name	WP8 effort
1 - ED	
2 - ICCS	
8 - JAS	
Total	

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
D8.1	Quality Management Plan	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	3
D8.2	Final Project Report	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	36
D8.3	Periodic Progress Report	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	6
D8.4	Annual Report	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	12
D8.5	Periodic Progress Report 2	1 - ED	Report	Confidential, only for members of the consortium (including the Commission Services)	18
D8.6	Periodic Progress Report 3	1 - ED	Report	Confidential, only for members of the consortium (including the	30

List of deliverables

Deliverable Number ¹⁴	Deliverable Title	Lead beneficiary	Type ¹⁵	Dissemination level ¹⁶	Due Date (in months) ¹⁷
				Commission Services)	
D8.7	Annual Report 2	1 - ED	Report	Public	24

Description of deliverables

D1.1 Quality Management Plan (ED) M3
 D1.2 Final Project Report (ED) M36
 D1.3 Periodic Progress Reports (ED) M6,18,30
 D1.4 Annual Reports (ED) M12,24
 D8.1 : Quality Management Plan [3]
 Management for the quality assurance of the project
 D8.2 : Final Project Report [36]
 Final report at the end of the project.
 D8.3 : Periodic Progress Report [6]
 Periodic report of the project progress.
 D8.4 : Annual Report [12]
 First year report of the project.
 D8.5 : Periodic Progress Report 2 [18]
 Second periodic report of the project progress.
 D8.6 : Periodic Progress Report 3 [30]
 Third periodic report of the project progress.
 D8.7 : Annual Report 2 [24]
 Second year report of the project.

Schedule of relevant Milestones

Milestone number ¹⁸	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification
--------------------------------	-----------------	------------------	----------------------	-----------------------

1.3.4. WT4 List of milestones

Milestone number ¹⁸	Milestone title	WP number ⁹	Lead beneficiary	Due Date (in months) ¹⁷	Means of verification
MS1	Reference Architecture and components specifications	WP2	2 - ICCS	8	Completion of the reference architecture, and components technical and functional specifications
MS2	First version of all tools	WP3, WP4	6 - EVR	18	Completion of the first version of all system tools
MS3	Early version of the integrated prototype (limited functionality)	WP5	1 - ED	24	Completion of the early integration and development of the early integrated prototype with limited functionality
MS4	Final version of the integrated prototype and portable unit (full functionality)	WP5	1 - ED	30	Completion of the final integrated prototype and portable unit with full functionality
MS5	Evaluation report of final prototype pilot deployment and Best Practices	WP6	10 - HNP	36	Completion of evaluation report for the final prototype pilot deployment and best practices
MS6	Exploitation plan	WP7	6 - EVR	36	Completion of the exploitation plan

1.3.5. WT5 Critical Implementation risks and mitigation actions

Risk number	Description of risk	WP Number	Proposed risk-mitigation measures
R1	Risk to travelers private data related to the ADDS.		The video data will be transmitted via the internet during pre-registration will be protected from unauthorized interception by encrypted exchange of information methods.encrypted
R2	ADDS possibility to provide false alarm of miss.		

Risk number	Description of risk	WP Number	Proposed risk-mitigation measures
R3	Difficulty in collecting and analysing end-users requirements	WP2	The detailed methodology to be developed in Task 2.1 will describe how to collect and analyse the relevant data. Partner's expertise also reduces the likelihood of this risk; in case it occurs, the methodology will be redesigned and simplified.
R4	Requirements of the pilot users are not aligned	WP2	Although the border control addresses similar problems, in case this risk occurs the project will address the common and generalizable requirements.
R5	HD data stream overloads Silent Taker classifiers, affecting real-time performance	WP3	

Risk number	Description of risk	WP Number	Proposed risk-mitigation measures
R6	Internet or radio connectivity fails	WP3	
R7	Low ability of through-the-(metal)wall hidden human detection	WP3	
R8	RBAT thresholds are not optimal	WP4	RBAT thresholds will be defined and tested iteratively in order to arrive at the optimum. It is possible however, that even during the tests several additional tests will be needed to ensure their values. This is why the tool foresees ways to review the risk estimation procedure and change the values of the thresholds.
R9	Integration is too complex and time consuming	WP5	The integration plan will be developed in parallel to the system design. The aim is to understand the potential complexity and risks as early as possible to

Risk number	Description of risk	WP Number	Proposed risk-mitigation measures
			develop the integration plan accordingly. In addition we will setup a continuous integration environment before the actual software development starts. This will allow to have daily software builds with automatic test cases in order to identify bugs and issues as early as possible.
R10	Users feedback is poor	WP6	Components will be further developed to accommodate the feedback. These components will be removed from the final version.
R11	Cultural Objections	WP6	Some religious/ cultural groups are resistant to being photographed. Also in Islam women generally wear a Hijab which covers the head and chest. Some variants require more covering such as the Niqab face mask or the full Burka. Mitigation: The standard Hijab should not prove too much of an obstacle, it does not hide facial features but may obscure head movements. iCROSS architecture could be trained to work specifically with Hijab wearers. Niqab and Burka pose serious problems. These are common to most other forms of traveller screening. The current fall-back is to deal with these travellers manually, using respectful and sensitive procedures. We expect this to be the case in the iCROSS solution. WP2, WP4 contribute knowledge for such mitigation strategies.
R12	“Conspiracy Theory” Objections	WP7	When any new technology is introduced the internet abounds with conspiracy theories such as “using the equipment increases your chances of getting

Risk number	Description of risk	WP Number	Proposed risk-mitigation measures
			<p>cancer.” There may also be data protection concerns on the part of travellers about how the data collected will be used. Firstly, the use of travellers’ own mobile devices will contribute to confidence about the safety of the process, Secondly, disclosure of copious information about the safety and security of the other technologies involved in the communication strategy will help to alleviate remaining fears. Finally, the privacy issues will be formally addressed and all necessary actions will be made.</p>

1.3.6. WT6 Summary of project effort in person-months

	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	Total Person/Months per Participant
1 - ED									
2 - ICCS									
3 - STR									
4 - MMU									
5 - ITTI									
6 - EVR									
7 - BIO									
8 - JAS									
9 - LUH									
10 - HNP									
11 - PBG									
12 - TRA									
13 - BSG									
Total Person/Months									

1.3.7. WT7 Tentative schedule of project reviews

Review number ¹⁹	Tentative timing	Planned venue of review	Comments, if any
RV1	18	tbd	mid-term review
RV2	36	tbd	final review

1. Project number

The project number has been assigned by the Commission as the unique identifier for your project. It cannot be changed. The project number **should appear on each page of the grant agreement preparation documents (part A and part B)** to prevent errors during its handling.

2. Project acronym

Use the project acronym as given in the submitted proposal. It can generally not be changed. The same acronym **should appear on each page of the grant agreement preparation documents (part A and part B)** to prevent errors during its handling.

3. Project title

Use the title (preferably no longer than 200 characters) as indicated in the submitted proposal. Minor corrections are possible if agreed during the preparation of the grant agreement.

4. Starting date

Unless a specific (fixed) starting date is duly justified and agreed upon during the preparation of the Grant Agreement, the project will start on the first day of the month following the entry into force of the Grant Agreement (NB : entry into force = signature by the Commission). Please note that if a fixed starting date is used, you will be required to provide a written justification.

5. Duration

Insert the duration of the project in full months.

6. Call (part) identifier

The Call (part) identifier is the reference number given in the call or part of the call you were addressing, as indicated in the publication of the call in the Official Journal of the European Union. You have to use the identifier given by the Commission in the letter inviting to prepare the grant agreement.

7. Abstract

8. Project Entry Month

The month at which the participant joined the consortium, month 1 marking the start date of the project, and all other start dates being relative to this start date.

9. Work Package number

Work package number: WP1, WP2, WP3, ..., WPn

10. Lead beneficiary

This must be one of the beneficiaries in the grant (not a third party) - Number of the beneficiary leading the work in this work package

11. Person-months per work package

The total number of person-months allocated to each work package.

12. Start month

Relative start date for the work in the specific work packages, month 1 marking the start date of the project, and all other start dates being relative to this start date.

13. End month

Relative end date, month 1 marking the start date of the project, and all end dates being relative to this start date.

14. Deliverable number

Deliverable numbers: D1 - Dn

15. Type

Please indicate the type of the deliverable using one of the following codes:

R	Document, report
DEM	Demonstrator, pilot, prototype
DEC	Websites, patent filings, videos, etc.
OTHER	
ETHICS	Ethics requirement

16. Dissemination level

Please indicate the dissemination level using one of the following codes:

PU Public
CO Confidential, only for members of the consortium (including the Commission Services)
EU-RES Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
EU-CON Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
EU-SEC Classified Information: SECRET UE (Commission Decision 2005/444/EC)

17. Delivery date for Deliverable

Month in which the deliverables will be available, month 1 marking the start date of the project, and all delivery dates being relative to this start date.

18. Milestone number

Milestone number: MS1, MS2, ..., MSn

19. Review number

Review number: RV1, RV2, ..., RVn

20. Installation Number

Number progressively the installations of a same infrastructure. An installation is a part of an infrastructure that could be used independently from the rest.

21. Installation country

Code of the country where the installation is located or IO if the access provider (the beneficiary or linked third party) is an international organization, an ERIC or a similar legal entity.

22. Type of access

VA if virtual access,
TA-uc if trans-national access with access costs declared on the basis of unit cost,
TA-ac if trans-national access with access costs declared as actual costs, and
TA-cb if trans-national access with access costs declared as a combination of actual costs and costs on the basis of unit cost.

23. Access costs

Cost of the access provided under the project. For virtual access fill only the second column. For trans-national access fill one of the two columns or both according to the way access costs are declared. Trans-national access costs on the basis of unit cost will result from the unit cost by the quantity of access to be provided.

History of Changes

Version	Date	Source	Change Description
		Comment from ESR However it is not clear why the deployment of the hidden human detector tool (not required by the topic) is included in the Proposal.	Section 1.3.4b/ "Hidden Human Detection Technology": Explanation provided on the rationale for the concept of Hidden Human Detection technology.
		Comment from ESR. However the case study on refugees on the Greek/Serbian/Hungarian land borders is not sufficiently contextualised and it causes confusion -the proposal establishes a link between the arrival of refugees in recent months in this region and the iCROSS technological solution but does not adequately acknowledge the fluidity of current and unfolding refugee situation in Europe.	Section 1.3.1: Explanation added.
		Comment from ESR However, providing wi-fi hotspots for connecting to the system is technically trivial, but the rationale for its uptake is not sufficiently demonstrated.	Section 1.3.4b/ "Wireless Technologies for Border Check Process": Explanation Added.
		Comment from ESR One shortcoming is that the affordability of the technology is not adequately explained.	The relative analysis will be considered in the WP 7. A relative statement has been added in the WP description.
		Comment from ESR Some of the resources that are not sufficiently detailed, for example the pilot train case, avatar, consumables and equipment.	Section 3.2/ "Resources to be committed"/ "Justification of resources and budget"/ "C. Equipment", "D. Consumables" & "F. Other costs": Relevant explanations are provided.
		Comment from ESR However, the proposal heavily relies on automated deception detection which poses certain risks that are not adequately addressed.	2 more risks have been added in the risk table in Part A.
		Comment from Ethics committee Include Ethics requirements and relating description of action	Section 5, Section 3.2/ "Project Bodies and main Roles": Ethics requirements, relating deliverables and description of action have been added.
		Comments from Scrutiny committee	Section 6, Section 3.2/ "Project Bodies and main Roles": Comments by Scrutiny committee have been added.
		Comment from Financial Officer	Section 3.2/ "Resources to be committed"/ "Justification of resources and budget": Tables have been added/updated for more detailed justification of costs

Contents

SECTION 1. EXCELLENCE.....	3
1.1 OBJECTIVES.....	3
1.2 RELATION TO THE WORK PROGRAMME.....	6
1.3 CONCEPT AND APPROACH.....	8
1.4 AMBITION.....	25
SECTION 2. IMPACT.....	34
2.1 EXPECTED IMPACTS.....	34
2.2 MEASURES TO MAXIMISE IMPACT.....	38
A. DISSEMINATION AND EXPLOITATION OF RESULTS.....	38
B. COMMUNICATION ACTIVITIES.....	44
SECTION 3. IMPLEMENTATION.....	48
3.1 WORK PLAN — WORK PACKAGES, DELIVERABLES AND MILESTONES.....	48
3.2 MANAGEMENT STRUCTURE AND PROCEDURES.....	52
3.3 CONSORTIUM OVERVIEW - INDUSTRIAL INVOLVEMENT AND VALUE CHAIN COMPLEMENTARITY.....	55
3.4 RESOURCES TO BE COMMITTED.....	57
SECTION 4: MEMBERS OF THE CONSORTIUM.....	60
SECTION 5: ETHICS AND SOCIETAL IMPACT.....	98
SECTION 6: SECURITY.....	127
6.1 SECURITY ASPECT LETTER.....	127
6.2 SECURITY CLASSIFICATION GUIDE.....	127
6.3 SECURITY STAFF.....	127
6.4 OTHER PROJECT-SPECIFIC SECURITY MEASURES.....	128
ANNEX.....	129

Section 1. Excellence

1.1 Objectives

The main objective of iCROSS is to **enable faster and thorough border control for third country nationals crossing the land borders of EU Member States (MS), with technologies that adopt the future development of the Schengen Border Management.**¹ iCROSS includes software and hardware technologies ranging from portable readers and scanners, various emerging and novel subsystems for automatic controls, highly reliable wireless networking for mobile controls, and secure backend storage and processing. **iCROSS designs and implements a comprehensive system that adopts mobility concepts and that consists of a two-stage-procedure, designed to reduce cost and time spent per traveller at the border crossing station.** The project envisages an optimal mixture of an enhanced but voluntary form of a Registered Traveller Programme (RTP) and an auxiliary solution for the Entry/Exit System (EES) based on involving bona fide travellers.

Continuous traffic growth, combined with the increased threat of illegal immigration, is putting nowadays border agencies under considerable pressure. Slow border crossings impact traveller satisfaction, business and trade. According to the Cockfield Report in 1980, the estimated income from abolishing controls on internal borders gave a rise as much as 2.5% of the annual GDP of the Member States. Calculating with figures from 2011, this means 232 billion EUR annually. A smaller, but still considerable rise in the EU GDP can be achieved through better facilitating border checks – and so, commercial traffic – at external borders. At the same time as making the border clearance process as streamlined as possible, the authorities need to make checkpoints safe and secure but also consider the limitations coming from human resources. Border checks become increasingly more challenging due to increased international trade, more complex supply chains and more sophisticated criminal activity. They also need to do all this at lower cost.

iCROSS focuses on the land border crossing points: road, walkway, train stations. It addresses the better facilitation of thorough checking required for third country nationals that intend to cross EU borders. To this respect, iCROSS specific objectives are:

- To **significantly increase the efficiency in terms of traveller throughput** at the border as well as security in terms of significantly fewer successful illegal crossings;
- To achieve greater comfort, **reduced time at the border** by utilising the portable traveller devices and portable units;
- To utilize **pre-registration step** as a means to better inform travellers of their rights, the procedures they will have to go through for their travel, the data collected and how they are analysed as per EU and national legal requirements and to obtain, where necessary, an informed consent from the traveller.
- To **reduce the subjective control and workload of human agents and to increase the objective control** with automated means that are non-invasive and do not add to the time the traveller has to spend at the border;
- To **create of a fifth tier** for the four-tier access control model of the Integrated Border Management System involving bona fide travellers, especially regular travellers into a Schengen-wide frequent traveller programme including a reward system based on number of successful crossings and trouble-free stay.

As mentioned above, iCROSS system consists of a two-stage procedure that includes the following:

First Stage (1) the registration before the travel to **gather initial personal, travel document and vehicle data, perform a short, automated, non-invasive interview with an avatar, subject to lie detection** and link the traveller to any pre-existing (at the authorities) data. Utilizing advanced multifactor analytics and risk based approach the data registered by the traveller is processed but also correlated with publicly open data (i.e. social media profile, google search etc.) or external systems such as the Schengen Information System (SIS II). Processing will need the travellers consent and they will be granted access to SIS II data related to their person and belongings as set in EU legislation and national law (exercising the fundamental right of freedom of information).²

Second Stage (2) the **actual control at the border** that complements existing (pre-registered) information with results of security controls that are performed with a **portable, securely wireless connected, iCROSS unit** that can be used inside buses or trains or at any other point. Multiple technologies check validity and authenticity of various parameters within travel documents, visa, face recognition between traveller and passport picture; real-time automated non-invasive lie detection in interview by officer, etc. The wealth of data and links collected are encrypted,

¹ See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP) - COM/2013/096 final - 2013/0060 (COD)

² Articles 41-43 in Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II). For national legislation please see example of 26.§ of the Hungarian Act No. CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System.

securely transferred and analysed in real time, providing an automated decision support system for the border control officers.

These procedures are separated based on two important criteria:

- (i) Information that the traveller can easily provide to the system with commonly available equipment of the portable devices or home based office equipment (scanner, photo camera, etc.) and
- (ii) estimated needed time for the integrated system to capture and process the necessary information i.e. capturing of video-audio conversation with an avatar for deception detection requires at least a few minutes conversation that should not delay the actual border control.

The two stage procedure enables multiple processing and cross-correlation of data and consultation with external systems without the pressure of delaying people, or vehicles from continuing their journeys. Travellers crossing the border with their own vehicle have to register their vehicle information.

Travellers' legal rights are addressed both at the European as well at the relevant national levels when collecting, storing and processing relevant data through the iCROSS legal framework. It is underlined that the participation in is not compulsory, it works on a voluntarily basis, offering ease of control for travellers willing to cooperate with authorities to speed up the border control.

The process incorporates novel mobility concepts, including the use of traveller's personal computing devices and sensors built into them to collect data at the pre-registration stage and dedicated secure devices at the border crossing to validate and further assist border guards in their decisions. These include face pictures, scans or pictures of all available and relevant travel documents and other data. The traveller will be informed about other documents to be requested at the border crossing (e.g. marriage certification, work contract, certificate of admission to school etc.). The traveller may also provide travel plan (time and place of entry), so that the authorities can better manage resources and diminish waiting time.

Based on the above, iCROSS addresses the main and specific objectives by research which has a dual focus:

- (a) **theoretical**, in terms of defining legal and functional requirements, novel border control concepts – for example a fifth tier to the four-tier access control model³ - and technologies as well as the controlled parameters and their contribution to the dynamic, intelligent, integrated risk assessment module enhancing the Common Integrated Risk Analysis (CIRAM) model currently in use. In particular risk factors will be defined to address the cumulative (based on multiple automated tools) estimated degree of malicious intent, involvement or intention of illicit activity, and real time detection of falsified, invalid, or mismatching of traveller travel documents, empowering the human agent to make more accurate decisions during border control operations, and
- (b) **applied**, whereby the technologies will be developed, integrated, deployed and validated with relevant robust quantifiable risk factors to ensure reliability, effectiveness and speed of border checks.

iCROSS integrated system provides automation of multiple key border control tasks which are organised in the following steps:

- A. **A pre-arrival registration and preliminary check of entry and stay requirements** where the traveller has to provide certain information before travelling and includes two phase:
 - (a) the registration of traveller related information (i.e. personal identification, travel documents),
 - (b) answer a set of questions about how they obtained their documents and their travel intentions, and
 - (c) the registration of trip related information (i.e. e-tickets, visa, etc.).
 Registration must be personal, as from 2006 the one-travel-document-per-holder is a general policy (see EC Regulation 2252/2004 Art. 4, section 3).
 The pre-arrival check results into a risk classification of each traveller that ranges from low to high. The travellers receive a personal notification (i.e. QR code) to their mobile device to facilitate the actual control to fast and easily retrieve the processed information and guide the next steps at the border crossing station.
- B. **The humans border control at the crossing station.** In line with the Schengen Border Code regulations, all travellers have to undergo border control when crossing the external borders of the Schengen Area. EU citizens and their family members undergo a minimum check, while third country nationals undergo a thorough check that complement the preregistered information. The personal code, generated at pre-arrival control phase, is used for fast retrieval of the traveller's processed information at the crossing point and guides the next procedural controls necessary. The minimum additional control will need just one biometric authentication and travel document scanning to verify that the person is the one that is holding the travel documents at hand, while the maximum control will use all the control functions offered.

³ The four tiers of the model are:

- activities in third countries, countries of origin and transit
- bilateral and international cooperation (cooperation with neighbouring countries)
- measures at the external borders
- activities inside the territories. (Council 2002a: 11)

C. Traveller's **vehicle control**. Currently during actual border control vehicles have to be checked for being illegally transported or stolen with manual check for condition (damages, missing parts, tires, the vehicle's cabin (passenger cab), trunk and the engine bay, with additional option of searching the entire vehicle (including partial disassemble) for drugs and illicit goods. On the other hand for cargo trains specific respective control procedures are dictated as well. However, in the majority of the cases and depending on traffic flows, vehicles or trains (passengers or cargo) are not systematically checked for hidden humans. The vehicle control also includes a search for vehicle identification (type, colour, VIN, number plate) in the Schengen Information System, verification of vehicle insurance and driving license of the driver, which could be part of the iCROSS vehicle pre-registered control. In some countries, the vehicle is also registered in the national entry/exit system. In this context, complementing the vehicle pre-registered control, during actual border control the iCROSS project provides the additional option the vehicles or compartments (e.g. in trucks or cargo trains) to be checked for hidden people with portable or deployable modules (based on radar and acoustic/sound sensors). This option is meant to test and prove integration ability and operation applicability; paving the way for future inclusion of potentially portable devices of other technologies used both for hidden humans or illicit goods detection.

Direct interaction between the authorities and the pre-registered travellers is enabled during all stages to exchange information (notifications about upcoming checks, waiting time, rewards and honours, rights and obligations in destination country, remaining days of stay etc. This system also facilitates notifications and alarms for the authorities as well for the traveller allowing the traveller to act in time, (i.e. when a traveller visa expires, etc.), thus avoiding a wasted journey through refused entry or expulsion. It also enables a deep interview with the traveller before travelling, enabling better specialization for border guard personnel and less waiting time at border gates for *bona fide* travellers.



Furthermore the following systems are included:

- I. A **securely accessible web interface** will be provided for travellers to register and guide them to provide the required information for the pre-arrival control. This will be presented in the form of workflow that shows the steps and the progress in the procedures and is executed at the backend by cloud infrastructure with enhanced security.
- II. A **portable hardware iCROSS unit will be devised including:**
 - a) **dedicated portable travel document scanners** to capture the travel documents (e-tickets, passports, ID cards, etc.) State of the art and off-the-shelf document readers and scanners with advanced features such as UV scanning will be integrated etc.
 - b) **biometric scanners** that capture state-of-the-art biometrics such as fingerprints, faces, veins, etc.
 - c) **portable modules** based on radar and acoustic sensors **to facilitate hidden human detection (HHD)** within vehicles, trucks or closed compartments triggering a more thorough inspection on a secondary level
 - d) **body mounted cameras**, based on those currently in use by police officers to monitor compliance with professional standards, **in this case to capture and process non-verbal features required for lie detection at the crossing point.**

- e) **the battery pack** which supplies electricity for all set elements. It can be also considered as a back-up power while working in the operating area.
- f) **touch screen** showing **information obtained** in the course of border control.
- III. Automatic **Deception Detection System (ADDS)**, which analyses Non-Verbal Behaviour (NVB) will provide an estimated level of deception based on analysis of the video-recorded question-answer session. Questions will be unpredictable by the traveller will target issues based on the traveller's data and profile analyses. For example questions will target assessing deception attempts by third country nationals entering the EU as economic migrants and engaging in terrorism, human trafficking and drug smuggling. These risk factors will also be passed to the human border agent, who will be supported by ADDS at the border crossing.
- IV. **Document Authenticity Analytics Tool (DAAT)**, which performs straightforward verification of travel documents. Building on top of existing systems (iFADO) the aim is improve response speed and efficiency.
- V. The provision of **Biometric Analytics (BIO)** that process the biometrics captured by the related devices of the portable hardware unit, etc., already included in the e-Passports of many countries, but also emerging and promising ones that enhance the security of the procedures (iris, vein, etc.)
- VI. The **Face Matching Tool (FMT)** that captures the face of the traveller at each stage and correlates it with the one in the travelling documents to estimate the probability that the travel document belongs to the traveller and that the same person completed the pre-arrival registration stage. With e-passports increasingly adopted this matching is further facilitated and addresses more efficiently variations and discrepancies such as aging, lighting, occlusion due to glasses or facial hair, etc.
- VII. **Vehicle Control Module (VEHC)** which will control and process the vehicle registration against cloning, alteration, theft and unauthorized use as well as status of international insurance bond.
- VIII. The **iCROSS integrated automated border control Risk-Based Analytics Tool (RBAT)**, will utilize state of the art risk based approaches to intelligently fuse all data collected and risk estimated and classify travellers to facilitate the human agent task.
- IX. A **human border control portable Agent User Interface (AUD)**, to visualise in real time the quantified metrics resulted from the sub-system analytics, guide the processing required and allow the agent to correlate the result with his own perception of the traveller.
- X. **Intelligent Border Control Analytics Tool (BCAT)** that performs analyses utilizing advanced computational intelligence based approaches in order to evaluate the performance of iCROSS systems discovering key patterns in the data that would help quickly identify False accept or false rejects of travellers based on the data collected in the Pilot study. The BCAT will use advanced algorithms based on machine learning, neural networks as well as statistical approaches to determine the confidence in the produced results.
- XI. **Wireless connectivity with ensured QoS will be provided through a high reliable radio network, involving wireless mobile and satellite access techniques**, by addressing respective Physical layer and Radio Resources Management challenges, with Optimum synergetic radio networks design, including scenarios with high speed vehicles (bus, trains, etc.), Analytical end-to-end models for the evaluation of cooperative transmission techniques and Development of a new unified resource management framework as well as relevant algorithmic solutions for coordinating and optimizing user access to ultra-dense networks.

Legal and ethical issues will be systemically considered to enable legal compliance with privacy, non –disclosure of sensitive information related to current and potentially future border control procedures, and legal training in issues related to the use of automated systems involved in border control tasks.

Real life experimental evaluation with both border guards and travellers across 4 European countries iteratively, covering a large scale of diverse requirements for land border control (bus, train, vehicles, pedestrian, etc.) with human border control experts and travellers will enable the validation of the proposed technology. Key performance metrics will not only focus on *False Accept rate* and *False Reject Rate of illegal travellers* but also on monetary (acquisition and maintenance), time, effectiveness and reliability associated with each task.

Dissemination of the project outcomes to key stakeholders, including border control and policing institutions, key policy makers and researchers in border control related issues and **to facilitate further research and new market opportunities** towards the border control research community.

1.2 Relation to the work programme

The following table lists how each of the presumed border control abilities as listed in the call topic BES-05 is addressed in the iCROSS Platform proposed solution:

BES 5 topic	iCROSS Platform proposed solution
Border control is likely to face increasing demands for efficiency, implying need for	iCROSS focuses on enhancing operational conditions at the border crossing stations in terms of:

<p>technical systems that are user friendly and reliable in operational conditions.</p>	<ul style="list-style-type: none"> • efficiency and accuracy, reducing time needed at the border crossing stations due to the iCROSS secure agent mobile system that allows faster and more accurate processing of the required information and the inclusion of pre-arrival control phase. This supports the efficient use of border control personnel by empowering them to utilize state of the art technologies to perform their duties while reducing subjectivity and human errors. • user-friendly human empowerment, is ensured by the use of web technologies familiar to the traveller, with a user friendly intuitive web interface to get informed about their rights, provide consent and provide data. The border agent portal will share on the same design and technology benefits but will be protected through a secure intranet system empowering agents by: <ul style="list-style-type: none"> ○ Providing direct access to traveller data ○ Providing decision support based on advanced analyses of traveller data including targeted issues the traveller needs to be further examined for. ○ Providing metrics derived from specific components of traveller's data. ○ Providing overall metrics for border crossings, including number of travellers expected to cross based on predictions derived from pre-registration information and correlation with past similar occurrences. • the incorporation of pre-arrival control for reducing actual border control, the portable control unit that removes the burden of getting out of vehicles and delays in travelling times, the possibility of continuous interaction between the traveller and the authorities, and the reward system, shaped after the current trend of gamification, transforming traveller risk analysis into a special treat, making frequent and benevolent travellers proud of their achievement. • reliability in operational conditions is ensured by the iCROSS scalable design and that a large part of the control, which burdened the operational IT infrastructure, will be done in advance, saving operational resources. Furthermore the ability of the system to warn in advance border control authorities of border crossing traffic will further help better manage resources.
<p>... use technology from adjacent markets such as mobile or satellite telecommunications, could help the costs of processing down to a minimum. In particular, the use of passengers' personal mobile devices is expected to enable efficient and reliable identity checks through the application of biometric technology...</p>	<p>With the iCROSS Platform, travellers will mainly use their own devices for pre-arrival check, saving resource in terms of operational lifetime of border guard equipment, which can accumulate to a significant saving in money, corresponding to the entire Schengen Area.</p> <p>Deployment of state-of-the-art biometric technology and the ADDS will result in reliable identity checks and efficient traveller risk assessment.</p> <p>Furthermore the prescribed QoS of the wireless connectivity will be guaranteed using, in an optimum combined and synergetic way, the transmission capabilities and the technological advances that are offered from mobile and satellite telecommunication networks. More specifically, iCROSS addresses this issue through the efficient and cost effective design of the radio network by taking advantage of the radio environment (propagation conditions, switching between technologies, optimum installation of radio relay nodes, antenna diagram and power allocation optimization, cooperative strategies etc.) and finally by minimizing the total energy consumption.</p>
<p>The ability to automatically and rapidly detect document forgeries is also expected to be further improved.</p>	<p>Several novelties are proposed for the automated and rapid process of document forgeries. Documents not only concern the official travel documents (passports, visa, etc.) but also other documents, such as tickets, vehicles ids, etc. There is the two stage procedure that allows multiple checks and cross-correlation with external systems. Furthermore, the integration of the FMT to calculate the probability the passport holder is the person depicted in the passport. Connected to the iFADO software, the DAAT will be able to detect forgeries initially at pre-arrival phase with the use and control of visible security features (MRZ checksums, OVI, iris printing etc.) and more detailed with reduced needed time at the crossing point in a mobile version with improved features in accuracy and time. The RBAT elevates the process and security to new levels, by calculating a cumulative risk factor for each specific traveller.</p>
<p>.. novel concepts relying on the use of traveller's personal mobile devices, and/or border</p>	<p>iCROSS is designed by involving border control experts who, after reviewing current procedures and requirement studies, as well as the state of the art on how to address each requirement using novel technologies, incorporated these technologies into the iCROSS platform. The technologies make use of personal web accessible mobile devices at the</p>

authorities' specific mobile equipment, for high security level passengers' identity control. ...biometric identification of travellers inside vehicles (cars, bus, trains as well as pedestrians). Portable Automatic Border Control (ABC) gate for land boarder (could be used at lanes outside the terminal)	pre-registration phase expanding the data availability per subject and enabling especially in the case of no risk frequent travellers the quick crossing while highlighting both the high risk travellers as well as the reasons for that assessment. With this new approach we engage bona fide travellers and ease their border crossing as well as creating an individual traveller risk assessment method never seen before. The iCROSS secure mobile agent unit will be developed incorporating secure wireless connection with guaranteed quality of service (QoS) allowing the agent to perform the complete additional check and have access to all pre-existing traveller information and decision support inside vehicles (buses, trains, cars, or for pedestrians) without delays and procedures requiring people disembarkation, manual processing. Advanced biometric sensors will be built into the unit (body mounted camera for face and deception recognition, fingerprint, palm vein) to enable the mobile collection of data empowering the agent to make quick and accurate decisions. A specific use case for the train travel will demonstrate how the control can be executed during the actual train travel without stop between the two train stations that connect the border.
Novel technological solutions and procedures to manage relevant associated workflows (to be validated by border guards in a realistic operational scenario)	iCROSS is designed around the existing border control workflows expanding relevant nodes with state of the art technology. The entire system results in a complete re-engineering of the procedures enabling robust automated border control, that includes steps for the traveller to provide requested information starting from the pre-arrival phase, dialogues to engage in video-audio conversion providing higher security levels, and procedures that decide and guide the border control at the crossing station based on cumulative risk from the traveller. The process involve all the steps and procedures that guide the work of the agent. They will be validated in real operational scenarios depicting the variety of cases (train, vehicle, pedestrian, etc.) in 4 EU countries with border to countries outside EU.
Legal, ethical or social implications must be taken into account	iCROSS solutions will be developed in line with the European Charter of Fundamental Rights, the Schengen Border Code, the Visa Code, the Schengen Best Practice Handbook for Border Guards (through inputs from our end-users) and the Code of Conduct for Border Guards (issued by FRONTEX). Data protection legislation will be taken into account as well, including the Prüm Convention for facilitating data exchange between MS law enforcement agencies. Specific partner (LUH) is responsible to ensure that the system is designed to address all legal, ethical and social issues.
New opportunities for European leadership in European, international markets	iCROSS provides the opportunity for the partner industries to develop necessary solutions and products which have the ability to provide competitive advantage for European industrial partner internationally. Europe will rely on own technological expertise and will need not to adopt technologies from abroad.

1.3 Concept and approach

1.3.1. Rationale

"The story began in 1985, when five EU states decided to abolish internal border controls – the Schengen area was born. On a continent where nations once shed blood to defend their territories, today borders only exist on maps. A Europe without internal borders brings huge benefits to the economy as well, which shows how tangible, popular and successful the Schengen achievement is and the importance it has for our daily lives and for our societies. We need to preserve and reinforce this common achievement."⁴

Similar advantages can emerge from the efficient, harmonised and secure border crossing of external borders of EU. According to an EC General Directorate of Migration and Home Affairs publication⁵, as a whole non-EU residents contributed €271 billion to the economy when travelling to the EU in 2011, most of them being business travellers, workers, researchers and students, individuals with close family ties to EU citizens or living in regions bordering the EU. Every year, more than 700 million⁶ external border crossings take place at the EU borders out of which about a third are made by third country nationals. Moreover, these figures are continuously rising as a result of an increasingly interconnected world.

On the other hand, illegal human trafficking has constituted one of the major challenges to the affected EU member states and organs in charge of EU border security. EUMS & Schengen Associated Countries reported more than

⁴ EC leaflet "Europe without borders: The Schengen area", Directorate-General for Migration, Home Affairs and Citizenship

⁵ http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228_01_en.htm

⁶ "EU Border Security", Government Gazette, March 2013

280,000 detections of illegal border crossing⁷, which was twice as many as the previous record of 140,000 detections in 2011, the year of the Arab Spring. Out of these numbers, only in 2013, there were around 9,800 detections of migrants using document-fraud to enter the EU or Schengen area illegally⁸. Approximately 224,000 refugees and immigrants have arrived in Europe passing through the Mediterranean Sea since the beginning of year 2015, as announced quite recently (first week of August) by the United Nations High Commissioner for Refugees (UNHCR)⁹. Given the explosive increase of around 300% (in the first half of 2015 vs. same period of 2014) of the number of immigrants who entered illegally in Greece, the official reports evidence an “arrival” in Athens by an average of 1,200 immigrants per day. It is absolutely clear that the ultimate goal of all the above categories is the entrance to European and Schengen countries through the Greek land and train borders between Greece / FYROM and Bulgaria. Especially, the Greek / FYROM borders (Eidomeni/Geygeli check points of Greek/FYROM land and train borders) tends to be, recently, vastly crowded. And this goes further, more intensified, in the land borders of FYROM / Serbia and Serbia / Hungary forming a pathway of tragedy especially when a country has extensive land borders or uneven and hard geomorphology. This pathway is given in the following frame, in order to absolutely justify the selection of the specific pilot sites by the iCROSS project (described later in further detail).

Given the size of the conflicts along North African and Middle East, the numbers previously given are quite modest considering what’s next in respect to the size of the problem. *“It is clear that we need a new, a more European approach”* pointed out in a joint statement the relevant EU Officers, France Timmermans, first vice President of EC, Federica Mogherini Responsible for Commission’s foreign policy and Dimitris Avramopoulos, Commissioner of Immigration. The correct balance is inevitably needed for protecting and promoting mobility and travel on one hand, and on the other hand, the need to preserve a safe and secure area within the EU while respecting the highest standards of human rights. The “smart border” initiative is part of the EC agenda since 2008, where a more modern and efficient border management is proposed, in order to speed-up border crossing for regular travellers but also facilitate and reinforce border check procedures for foreigners travelling to the EU using the external borders.

It is obvious that the EU needs now, more than ever, new, user-friendly, mobile and reliable technologies to be adopted and customised accordingly for the border check process, so as to simplify life for foreigners frequently travelling to the EU and to better monitor third-country nationals crossing the borders. Mobile technologies and cloud-based services are rapidly changing the IT landscape, are assumed to be robust technological components and therefore can be taken under serious consideration when designing novel border management services. The same stands for the growing computational power and the low-cost mobile devices, smartphones, etc. *“the world is home to 7.2 billion gadgets, and they’re multiplying five times faster than we are”*¹⁰ - which can make new border management tools increasingly accessible to nearly every traveller and border agent, around Europe and the world. Most EU countries apply the same border control rules to non EU-citizens coming to the EU. Common rules make it easier for people coming to the EU. They are also important for the EU’s border-free travel zone throughout which authorised travellers can move freely without passport controls between EU countries.

To this end, having in mind that nowadays border control is like looking for a needle in a haystack and that most people crossing a border are law abiding and honest, iCROSS aims to implement a novel but “light-touch” processing for these people going through land borders. iCROSS combines portable and security-driven technologies to speed-up and automate the procedures, ending up finally to a robust mechanism for “moving the hay aside so that the needle is easier to find”.

Refugees’ pathway through Greek / Serbian / Hungarian land and train borders

The refugees in their vast majority arrive by bus or taxi from Athens at the border with FYROM in Eidomeni and Evzoni land borders. Illegal transfer was enormous in previous years, since they lodged in the forests and fields of the Greek borders waiting for the chance to enter the neighbouring country or were falling victims of exploitation and trafficking, paying handsomely for entering FYROM.

Thus, the illegal manner of the transfer was reduced due to governmental policies and political reasons and not because of technical aids and systems that could help a better classification; holistic systems like airport check points or technical aids of such character in some cases and in certain countries simply do not exist at the land borders. Buses and taxis disembark refugees in the neutral zone, a short distance from the station Eidomeni, where the Greek trains (TRAI NOSE) running route from Thessaloniki to Belgrade enters the territory of FYROM in sealed wagons, so if during the journey identify illegal passengers. However, in any case, the control is small, if

⁷ FRONTEX Annual Risk Analysis 2015

⁸ FRONTEX Annual Risk Analysis 2014

⁹ «Η ΚΑΘΗΜΕΡΙΝΗ της ΚΥΠΙΑΚΗΣ» Greek largest Sunday newspaper, printed and online editions of 9/8/2015, following press releases of the UNHCR and the Hellenic Police. <http://www.ekathimerini.com/>

¹⁰ The Independent article “There are officially more mobile devices than people in the world”, Zachary Davies Boren, 7-Oct-14

¹¹ «Η ΚΑΘΗΜΕΡΙΝΗ της ΚΥΠΙΑΚΗΣ» Greek largest Sunday newspaper, printed and online editions of 9/8/2015, <http://www.kathimerini.gr/826645/article/epikairothta/ellada/maxh-gia-mia-8esh-sta-trena-ths-fyghs> Article “Battle for a seat in the trains of great escape”, Stavros Tzimas, 9-Aug-15, <http://www.ekathimerini.com/>

at all, limited only to visual inspection by guards, occasionally or indicatively, due to the volume of people and the lack of technical aids that would help a smooth and fast operation.

Railway Station Gevgelija, a few hundred meters from the Greek border Eidomeni, refugees are struggling to board the train covering local routes to Skopje and Kumanovo on the other side of FYROM on the border with Serbia. Up to 500 people are packed into three or four old and small wagons on a route that in previous years had only a few passengers if anyone at all. Nowadays however, the "trains of the great escape" are carrying thousands of Syrians, Iraqis, Kurds, Afghans, on their journey to salvation. About 1,500 passengers travel daily into the city of Skopje and Kumanovo in the north, where they hope that they will pass secretly across the border into Serbia. Crews of Slav-FYROM police record them, providing a residence permit of 72 hours on the territory and transfer them through bus to the small railway station Gevgelija, to board the trains. Others, those who can pay "well", find coach or taxi to Serbia at Kumanovo in FYROM-Serbia borders. However, the passage in Serbian territory through wooded areas is not easy, as the authorities of the country follow a stricter policy, having developed strong police forces assisted by armed detachments of Hungarian, German and Austrian police and having set up "reception centres" in the Presevo Valley. Serbs, unlike Greece, FYROM and Bulgaria, do not follow policies facilitating transit flows for the additional reason that the refugees end up trapped at the Serbian – Hungarian borders. The borders with Hungary are the gateway to the final destination in West Europe and this time are considered to be the most "hot" zones of Europe in the refugee issue. Despite the strict measures there, thousands of people of all ages arrive (with the help of unscrupulous traffickers) near the town of Subotica, in order to go to Hungary. The fear of forests and plains of Vojvodina possibly being flooded with refugee crowds of Syrians and Iraqis scares both Serbs and Hungarians with the latter working feverishly to raise a steel fence of 170 km length in order to confront attempts of violent invasion, similar to that in Calais, France.



The situation described in the passage above, shows that the way of the refugees from Greece to western Europe includes the train trip through Eidomeni station. The train pilot was conceptualised to address this problem. According to preliminary analysis of requirements it was indicated that two issues arise during train trips:

1. the majority of people that want to travel through the borders illegally they board on the trains and hide there, since they don't possess all the papers for proper border check.
2. Those who do not hide and go through the process legally, follow the existing procedure of checking the papers within the train. The train stops at the border and the border police agent is boarding on the train and collects all papers and passports. He is bringing them to his office to check. When done he brings them back to the train and gives them to the passengers.

1.3.2. Project positioning in terms of Technology Readiness Level

The following figure illustrates the TRL of iCROSS technological components.

Project results in relation with TRL	TRLs at project start	TRLs at project end
Integrated cloud iCROSS system	-	5
ADDS	5	7
RBAT	6	7
DAAT	7	8
Biometrics (face, fingerprint)	7	8
Biometrics (vein..., iris)	4	5
Portable HW unit	-	5
Portable HHD unit (radar & acoustic sensors)	3	5

Fig 1: iCROSS TRL illustration

1.3.3. Previous research and innovation activities linked with the project

The project is well positioned in terms of the State-of-the-art, defined by research projects at European and international level, which have already been taken into account for their concepts and published results, and goes beyond national and international research projects with concrete opportunities for synergy or adoption of projects results, because of the existing contacts from the consortium which are listed below:

Project	Description	iCROSS relevance
FASTPASS FP7 SECURITY	FastPass establishes and demonstrates a harmonized, modular approach for ABC gates. Fastpass will serve both demands at the same time to keep security at the highest level while increasing the speed and the comfort for all	iCROSS goes beyond the results of FastPass by improved traveller identification technologies, such as new biometric modules, the ADDS, the portable HW and HHD units, the

	legitimate travellers at all border control points aiming at a minimum of privacy intrusion.	risk based approach, etc., will increase the security of the process and minimize spoofing.
ABC4EU FP7	ABC4EU identifies the requirements for an integrated, interoperable ABC system, respectful of citizens' rights, at EU level, taking account the future needs derived from the Smart Border and other EU and national initiatives and paying very special attention to citizen rights, privacy and other related ethical aspects. ABC4EU focuses in the need for harmonization in the design and operational features of ABC Gates, considering specially the full exploitation of the EU second generation passports and other accepted travel documents.	The ABC4EU system is of particular interest for iCROSS, and particularly its deployment in the real-life scenarios (not yet implemented), but goes further by introducing the pre-arrival phase, where much query time is preserved. Furthermore, innovative tools, such as the Avatar which, working with ADDS, will detect human stress and deception through face analyses, are adapted.
MOBILEPASS FP7	MOBILEPASS focuses on research and development towards technologically advanced mobile equipment at land border crossing points. Border control authorities can check European, visa-holding and frequent third country travellers in a comfortable, fast and secure way. The mobile solution incorporates new technologies needed in mobile scenarios and embeds them in the actual border crossing workflow to speed up control procedures.	iCROSS will consider this project results and will integrate any suitable approach. However, iCROSS goes far beyond by providing an integrated comprehensive environment, of which MOBILEPASS maybe an interesting component.
EFFISEC FP7 project	EFFISEC delivers to border authorities more efficient technological equipment for identity and luggage control of pedestrians and travellers inside vehicles, at land and maritime checkpoints, while maintaining or improving the flow of people crossing borders and improving work conditions of border inspectors, with more powerful capabilities, less repetitive tasks, and more ergonomic equipment.	iCROSS will consider the results of this project and will integrate any suitable approach, especially regarding to human/goods detection component and envisages of a more complete, integrated solution that will deal with all aspects of land border control.
TABULA RASA FP7 project	Analyses weaknesses of biometric identification process software in scope of its vulnerability to spoofing, diminishing efficiency of biometric devices. The goal is to provide more resistant systems and standards for protection of biometric devices against spoofing.	iCROSS will use results of TABULA RASA to protect the planned solutions against spoofing or impersonation.
eGate External Borders Fund, Hungary	The pilot deployment of an ABC system financed of Schengen External Borders Fund in Hungary at Budapest Liszt Ferenc International Airport in 2014.	HNP will share lessons learned, experience and results on use of ABC gates by travellers and time to pass compared to manual minimum check with other iCROSS members.
Next Generation VIS, Hungary	Supported by External Borders Fund, With the deployment of fingerprint readers for TCN control, this new system allows first line officers to check visa holder's identity with biometrics. HNP was participant of the pilot project aimed at testing the innovation for all MS.	HNP will share lessons learned, experience and results on use of new VIS technology including deployment experience to facilitate pilot deployment for iCROSS.
BEAT - Biometrics Evaluation and Testing SEC-2011.5.1-1	The BETA project implements a framework of standard operational evaluations for biometric technologies with an online and open platform to transparently and impartially assess biometric systems against validated benchmarks, create protocols and tools for vulnerability analysis, and develop standardization documents for Common Criteria evaluation. Moreover, the project deals with the legal implications connected with biometric devices. In addition, because of the influence of the results on the standards, decision-makers and officials will be kept up-to-date with the progress made in the field of biometrics.	iCROSS will consider the BETA project's results in the area of technology assessment. Particularly relevant will be the issue of arising legal implications with regard to state-of-the-art biometric systems, which can be taken into consideration in the iCROSS project.

1.3.4. The overall approach and methodology

a. Legal Compliance and legal Policy Makers synergy

Art. 7 and 8 of the European Union's Charter of Fundamental Rights declare the right to respect someone's private life and the protection of personal data as fundamental rights for everyone in the European Union. Data Protection and Respect to private life are therefore core values within the European Union. The importance of data protection and privacy of individuals have been further strengthened during recent years in particular through two judgements of the European Court of Justice. The first one declared the Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) invalid.¹² *The Court takes the view that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.*¹³

The second one declared (some kind of a) right to be forgotten against search engine operators. The data subject can demand that a search engine has to delete links to the data subject.¹⁴ Especially the judgment regarding the Data Retention directive shows that the processing of personal data through state authorities is not per se and necessarily compliant with fundamental rights in any case, even if it is foreseen to fight terrorism and crime. Nevertheless, the right to privacy can also be limited to ensure other (fundamental) rights which might be afflicted, like in the context of iCROSS the Right of Liberty and Security declared in Art. 6 of the Charter. Such limitations of the right for privacy or the protection of personal data could be set in relevant EU and member state legislation concerning border control measures, e.g. limitations to freedom of information in the Prüm Convention¹⁵. In a rather recent case, the CJEU declared the usage of digital fingerprints in identity-cards and passport-control scenarios as in principle compliant with European primary law and stated that national law does not necessarily have to exclude secondary usage of biometric data (CJEU, C-446/12 to C-449/12).

The use of technologies at the borders of the European Union, as proposed in iCROSS, enables state authorities to collect and process personal data, in the way that data subjects cannot deny the collection and processing of their data if they want to enter or leave the territorial of the European Union. Due to these circumstances, the proposed data processing cannot be justified on a basis of informed consent, but only on a legal basis which allows it. Systems like video and audio surveillance or additional data collection from other resources like social media without the knowledge of the traveller affect the rights of privacy and protection of personal data. Especially the collection of personal data by state authorities without the knowledge of the traveller, e.g. social media content, might not be allowed in every single member state based on its current laws. This might not be decisive in cases of publicly accessible profiles, as this kind of information might not fall within the scope of data protection regulations, but at the same time suggests new issues to be regarded, such as fake profiles which might affect the value of the information contained. Also state authorities may have specific restrictions and requirements concerning the use of hard- and software, like the use of cloud services. Therefore the project will investigate whether measures proposed by the project can be legally justified with the goal of improving cross border travelling as well as the work of border agents. It is understood that the project takes place in between the conflicting priorities of data protection and the need for national security, consequently between fundamental rights of individuals and the need to protect the general public. On these grounds, the project will firstly demonstrate the legal system of the EU and the implementation of relevant EU law by its member states. This will be followed by an analysis of the legal framework at European level and their transposition into the relevant member state law. Furthermore the relevant future legislations like the proposed Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union (COM(2013) 95 final) will be considered. This will be done in close cooperation with other European projects on crime prevention LUH was or is actively involved in such as CITYCOP, SMART and RESPECT.

Depending on these results requirements of a possible future legislation concerning the use of such proposed techniques will be evaluated and a conclusion given. A starting point will be an examination of the judgements of the European Court of Justice concerning the Data retention directive and the regulation to store fingerprints on travel documents. Furthermore there are several regulations and jurisdictions as well as bylaws on international and national level that will be assessed in respect to data protection and data security, for instance the Schengen acquis¹⁶, which

¹² ECJ, 8.04.2014, C-293/12 and C-594/12.

¹³ ECJ, Press release, curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

¹⁴ ECJ, 13.05.2014, C-131/12.

¹⁵ "Police Robots and the Prüm Convention - Compliance ..." 2015. 10 Aug. 2015

¹⁶ http://www.academia.edu/10208625/Police_Robots_and_the_Pr_Convention_Compliance_Study_on_Police_Robots_and_Freedom_of_Information

¹⁶ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33020>

has been concluded in order to create a safe situation in an area of open borders.¹⁷ Schengen area is now part of the legal and institutional framework of the EU. It is therefore an area of parliamentary and judicial scrutiny, and attains the objective of free movement of persons enshrined in the Single European Act of 1986.¹⁸ It has been founded by several Treaties, such as the Accession Treaty¹⁹, the Implementation Treaty²⁰ and the Prüm Convention that will be evaluated. Further the Schengen Border Code²¹, Visa Waiver Regulation, Visa Code, FX Regulation, European Border Guard Teams, EUROSUR Regulation, Biometric passport regulation and the directive on free movement will be analysed. Additional on these findings technical requirements will be proposed to protect personal data to comply with existing legislation and to minimize possible intrusions in the right to protect personal data and privacy.

iCROSS's Data Protection Framework will guarantee that the system development as well as the system deployed will work as privacy-benchmark in the area.

The project's data protection and data security framework will guarantee the non-disclosure of personal and/or other sensitive information related to current and potentially future border control procedures. In addition, legally sound best practices in the use of automated decision support systems in border control will be presented. Legal systems often require (in their data protection laws) that final decisions having an impact on citizens' rights are taken by a human and not a machine. iCROSS will allow a machine-human interaction that supports maximum efficiency without jeopardising the data subject's right to be subject of human decision-taking. iCROSS will build on work already undertaken in SMART²² and RESPECT²³, making use of the model laws developed there.

b. Technical approach

[REDACTED]

[REDACTED]

[REDACTED]

¹⁷ *Hufnagel, Harfield, Bronitt*, Cross Border Law Enforcement, Regional Law Enforcement Cooperation- European, Australian and Asia – Pacific Perspectives, p.112, Abingdon, Oxon 2012.

¹⁸ <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33020>, last viewed at August 12th 2015.

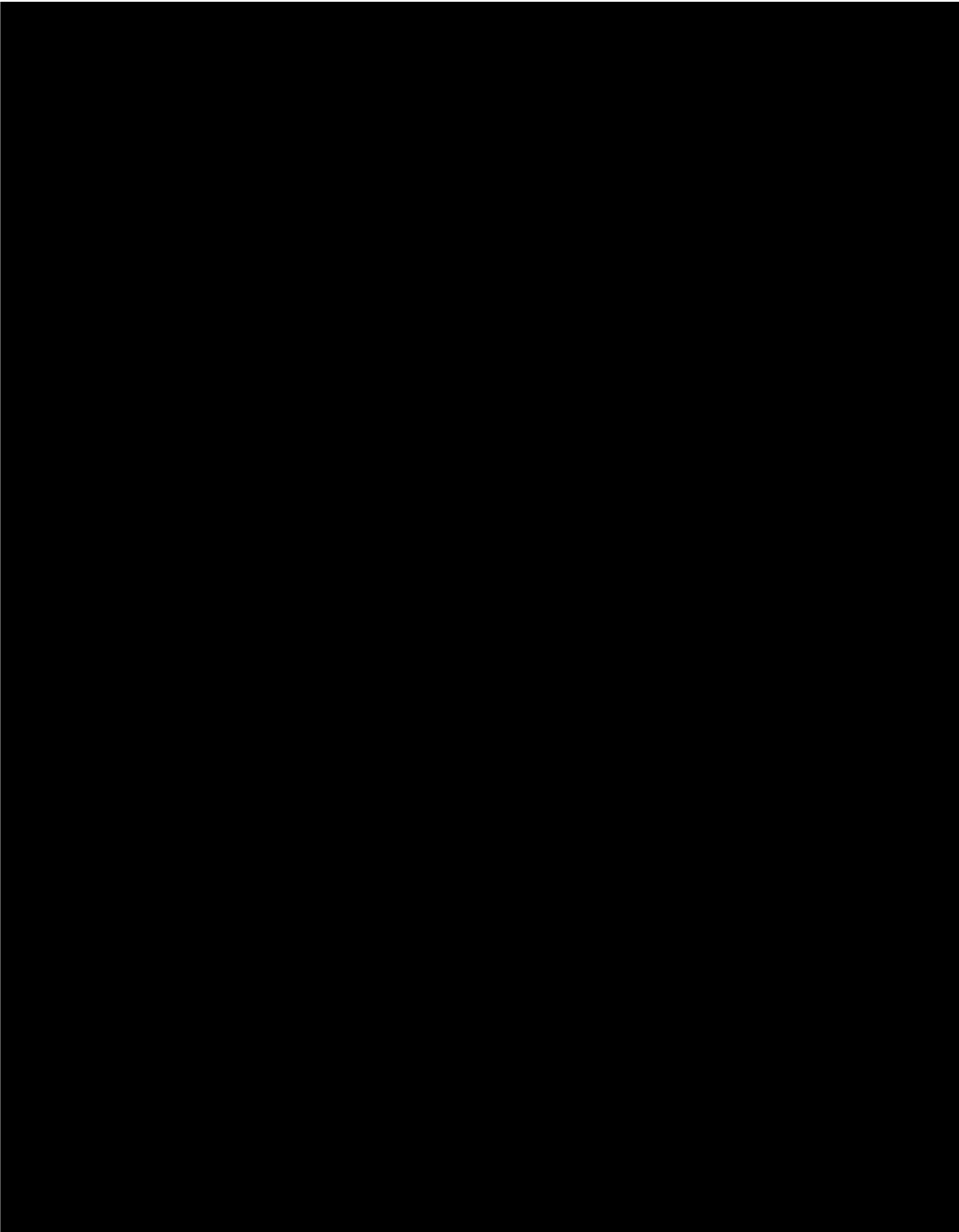
¹⁹ "EUR-Lex - 42000A0922(04) - EN - EUR-Lex." 2014. 10 Aug. 2015

²⁰ EUR-Lex - 42000A0922(02) - EN - EUR-Lex." 2014. 10 Aug. 2015

²¹ Regulation (EC) No 562/2006 - EUR-Lex - Europa." 2006. 10 Aug. 2015

²² http://smartsurveillance.eu/index.php?option=com_content&view=article&id=69&Itemid=64

²³ http://respectproject.eu/index.php?option=com_content&view=article&id=46&Itemid=73



The border agent avatar

Border control officer's tasks rely on bilateral human interaction such as border control agents interviewing an individual using verbal and non-verbal communication to both provoke response and interpret the traveller's responses. ADDS is powered by Silent Talker, a system capable of semi-automating that process by quantifying the probability of deception from the part of the interviewee. However, to maximize the potential impact of ADDS the border crossing, it would be beneficial to utilize this system not only to provide support to a human border control agent but also to collect data completely automated on the potential of deceitful behaviour by a traveller. To achieve this, an advanced verbal and non-verbal communication border control agent avatar will be created. This will be instantiated per traveller and will be personalized to correctly communicate with the traveller including utilizing subtle non-verbal communication cues to gauge response to them. The avatar will potentially improve performance in certain situations compared to a human agent because it will be able to correctly adapt to the travellers profile as well as be able to target specific interview topics of high relevance to specific travellers based on analyses of data available on them. Furthermore, completely automating parts of the interview questions will enable to shift some of those to the pre-crossing phase thus resulting in considerable time and monetary savings while increasing security. As part of the iCROSS evaluation the use of the avatar will be evaluated so that it can be determined what type of questions and to which travellers it responds better especially at the pre-crossing phase. This will ensure that full automation is only deployed when meaningful to do so while still enabling pre-crossing collected data.

The border control Agent User Interface AUI

Multiple visualization ways will be provided in order to manage the data captured by iCROSS platform, including both the pre-arrival as well as the border crossing phase. They will additionally present the results that the specific tools generate in order to assist border agents with interpreting and accessing the data in real time within their procedures during decision-making. Visualization of risk estimate that support decision of the human agent will provide a discreet output clearly visible and readily interpretable only by the agent.

The system aims to support queries and statistics extraction, that is particularly useful in case the agent needs to further investigate the reasons that automated risk estimations were high, or during special investigations. Finally, the system will incorporate and visualise information that are being recalled by external assisting databases, either the existing ones like SIS/VIS, credit/debit cards status, etc. or databases that will be available in the future, maybe by Interpol, Europol, etc.

Mobile Application

Mobility is one of the characteristics that iCROSS aims to adopt in its application. Therefore, it is of great necessity to reflect the interaction of the travellers and the border agent through iCROSS platform in a **mobile application**. This application will enable the travellers to rapidly recall information already uploaded to the system and will acknowledge them with the next steps or any parallel information needed before, through and after the border check procedure.

This mobile application is referring to all travellers, from different countries, different ages and cultures and should therefore understand the current practices and the desires of potential users, as well as the ways in which people experience or would like to experience life. A novel methodology for the design process will be followed, based on innovative research and literature printed out by the MIT²⁴, exploring the traditional user-centred design procedure, which is based on the user observation in their real context of use. iCROSS's new agile methodology will take into account the inability of mobile devices to observe users in many of their daily use of mobile applications and will travel far above the user-centred design procedure, by using creative methods in order to "analyse" users' interactions such as generative research²⁵ and structured interviews. **The ultimate goal is to create an entirely new experience with better communication and interaction.**

Document Authenticity Analytics Tool (DAAT)

The proposed DAAT will be built on top of an existing system, the ED's False and Authentic Documents Online (FADO) and its public version (PRADO). This system will be repurposed and customised to explore the knowledge and experience to provide an added value to fluent, fast and secure border crossings while ensuring security Schengen Handbook. The focus will be on increased performance for a more rapid and straightforward verification of travel documents in short time durations, especially during the check phase process. The implementation will take place in two stages, both in the pre-arrival/registration phase, as well as in the check phase.

²⁴ F. Bentley, E. Barrett, "Building Mobile Experiences", MIT Press, 2012

²⁵ "Communicating with mobile technology" class, Massachusetts Institute of Technology

²⁵ It is research that takes place in the form of discussion with end users in an approach to generate new design ideas (see above MIT references).

iCROSS tools will have the capability to interface in the future with national/international authorities', Europol's, Interpol's newly or future developed databases using the travellers' personal information, such as name, date-of-birth and nationality and thus may result in criminal detection of individuals attempting to carry out transactions using identity documents; real-time law enforcement notification; increased border agent safety by enhancing identity protection measures to reduce criminal activity and attacks.

Automatic Deception Detection System (ADDS)

A single, real-time, Silent Talker (ST) classification system will be developed for both pre-arrival and border crossing interviews. Based on existing (ST) architecture, this component will be re-engineered in a 6-phase procedure, as following:


B

Fingerprints

iCROSS intends to adopt fingerprint technology to improve the flow of travellers at border crossing in Europe. The overall approach is to integrate this technology within the iCROSS portable device used by every agent to check people's identity. Most travellers belonging to the EU and from developed countries are issued an e-passport which has an embedded RFID chip that carries digitally signed biometric information (our fingerprints normally, however they are incorporating palm vein data). Obviously, travellers coming from underdeveloped countries doesn't have their fingerprint registered on their passports, so this additional measure of security at border controls is orientated to speed up the flow of travellers owning the mentioned e-passports. When the people don't have the necessary biometrics integrated document, other ways will be used, such as to capture them from the visa issuing or the visa documents.

Palm vein

The BioSec palm vein based biometric identification system relies on the fact that the blood stream in the veins absorbs near IR light and the complete vein pattern becomes visible for the IR optics. The image created will be digitized immediately within the sensor and the image will be deleted irrevocably and an encrypted HASH code will be created. Any direct connection between the person and the biometric template will be terminated. The benefits of a HASH code is that it is always changing, is according to actual mathematical knowledge irreversible.

In opposite to other biometric authentication methods the palm vein recognition based biometric identification uses an "inner" ID, therefore the palm vein pattern cannot be seen from outside, cannot be copied or reproduced, like fingerprint. In order to avoid identification, fingerprints can be burned off with e.g. acid or tricked with spoofing. In order to avoid palm vein identification, you have to cut off your hand, which is less likely. Each time the matching procedure is a several step identification/verification procedure to ensure the FAR rate of 0,00008% (certified by BSI in Common Criteria 2 certificate).

The benefit is also the disadvantage, namely that palm vein based identification cannot be used for fight against crime, since you do not leave a trace, therefore palm vein identification forms an ideal combination with fingerprint and/or face recognition, since palm vein recognition has a better FAR and FRR rate and is ideal for primary

authentication but registering fingerprint and/or face templates create valuable databases for law enforcement organisations.

The largest reference for BioSec palm vein recognition based mass identification is the Groupama Arena, where the access control system is equipped with biometric authentication and the BioSec system can identify 23000 people within ~90 minutes at 36 gates. Successful matching takes place within 1 second. The importance of this reference is, since it proves that the system can be used by all types of people (young, old, male, female etc.) and the system does not slow down even in stress situation just like a mass entry before a soccer game. Right now more than 55 000 people are registered in the database and last year more than 250 000 entries have been managed without any security or system issue in outdoor conditions in the winter or summer.

Face Matching Tool (FMT)

The FMT System shown in Fig. 8 consists of 2 stages: pre-arrival and border crossing. At the **pre-arrival phase (where the person is at home or similar)**, two inputs will feed the check phase: (1) sample facial images of the traveller obtained during the interaction with the avatar/ADDs and (2) the passport that the traveller uploaded to the system. Therefore, a first “**offline**” verification will take place to compare the sample facial images of the person who talked with the avatar and the uploaded passport, to check whether it is the same person or not. Following that, at the **check phase (where the person is physically at border controls)** a second “**online**” verification will take place. It will consist of capturing facial images of a traveller and retrieving and comparing with the photo from the traveller’s documents, either stored in electronic version or scanned from the passport photo page. A high resolution camera detects and captures the facial image of the traveller in quality resolution for processing. A passport scanner scans the photo on the passport and an e-passport reader retrieves the electronic file of the photo stored (in the case of e-passport). Finally, before the result of “Match” or “No Match”, a **last verification** is done to check whether the person attempting to cross the border controls is the same person that talked with the avatar in the pre-arrival phase.

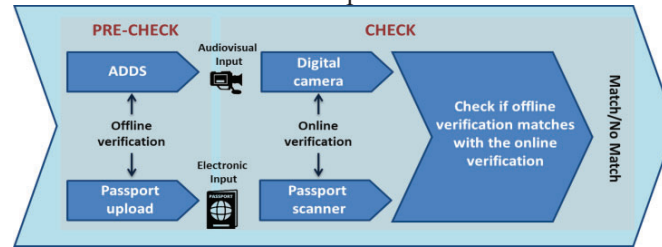


Fig 5: FMT System and Architecture

The first core of the **FMT Engine** compares the photos between uploaded, scanned and stored in the case of an e-passport to detect forgeries or mismatches between them. The different or reduced quality of the scanned image compared to the original photo image will be considered in the matching process, which extracts some start-of-the-art **invariant facial features** such as shapes, local patterns and biologically inspired features from the images.

The second core of the FMT Engine extracts both global and local **facial features** from the sample facial images obtained in the ADDs and from the high resolution images as well as facial features such as eyes, nose and mouth. Parallel matching processes take place between captured image and stored photo (or scanned in case of conventional passport) in global and local scales. The **global matching** provides a holistic verification including shape and geometrical information, while **local matching** further enhances the confidence of the matching with matched facial features.

The third core accounts for the tolerated **natural variations** in lighting, aging, expression and facial marks, built on training thousands cases. These changes are described by smooth, nonlinear **manifolds** extracted from the training samples. These changes exist in both global and local features and are treated coherently. Mostly importantly these changes are different from the discrepancies between subjects and are thus modelled differently to differentiate the **pixel and manifold differences**. The ability to recognise the manifold changes are the key to the robustness of the FMT System. The sensitivity of the system is influenced by the pixel difference, though other differences can help make informed judgement on the differences between the subject and the photo.

Finally the **Fusion** core of the FMT System synergises the matching in various scores and different levels and provides an overall matching score of the traveller and the passport photo. With a pre-set confidence level (set by the border controls), this overall score will translate to either “Match” or “No match” output to the Border Control System.

Regarding to where will the FMT engine is implemented at border controls, the overall concept is to integrate it in all traditional security cameras present as well as – a more innovative concept – to provide every agent with a shoulder-mount camera. This way, agents will not depend on traditional cameras, which are more orientated for monitoring and support, and will have their own camera to capture specific sample facial images of the traveller.

Cloud-based storage, processing and data protection

The processed information from all technological components (both during the pre-arrival and check phase) will be collected to a centralized cloud-based application that will allow the analysis and evaluation of travellers' risk, uploaded data and timestamped interviews. Moreover, the cloud based application will host the real-time statistics analysis tools. Border agent specific statistics will include login/logout time, location and terminal ID, number of passports and number of falsified passports found. Traveller specific statistics will include date/time of arrival, expected departure based on above, number of visits, frequency of visits, categorization of visits, and country of origin and destination country.

Processed information is securely stored and processed in the cloud, while complying to the **European data protection guidelines** and following industry best practices on **privacy and security**.

Secure access and secure transfer of the data from the cloud to border devices and vice-versa. An architectural decision will be made to determine the appropriate method to protect data when it is being transmitted. The most common options available are Virtual Private Networks (VPN) or a Secure Socket Layer (SSL) / Transport Layer Security (TLS) model. SSL 3.0 and TLS 1.2 for the web application and API is selected. At a minimum, all of the following should be followed:

- Require SSL for all pages. Non-SSL requests to these pages should be redirected to the SSL page.
- Set the 'secure' flag on all sensitive cookies
- Configure the SSL provider to only support strong (e.g., FIPS 140-2 compliant) algorithms
- Ensure that every SSL or TLS service uses a certificate that is valid, not expired, not revoked, and matches all domains used by the site. We should also schedule renewal of all certificates before they expire to ensure the services remain secure
- Backend and other connections should also use SSL or other encryption technologies
- Use SSL or TLS throughout the entire domain in order to reduce complexity. Remember that any included content such as images, JavaScript or CSS should also be provided over SSL or TLS in order to avoid 'mixed content' warnings in users' browsers
- Obtain an Extended Validation (EV) certificate

Secure Application Programming Interfaces. APIs are integral to security and availability of services. These interfaces must be designed to protect against both accidental and malicious attempts. Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities will be avoided at all times.

Access Right Management System and Relevant Policies

Authentication. The traditional form of security tokens like username/password used to access online services are prone to phishing attacks and hence do not provide complete security. Identity will be protected with directory integration, groups, as well as Single-Sign-On (SSO) integration. Authentication controls will include Two Factor Authentication (2FA), and session expiration.

Secure Management Interfaces. Command and control facilities are understood and secured. SSL will be used to encrypt all transactions.

The cloud-based system will follow a "Privacy by Design" principle in order to promote privacy and data protection compliance from the start. The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs²⁶), 'privacy by default' settings and the necessary tools to enable better protection of personal data (e.g., access controls, encryption). The principle of 'Privacy by Design' should be binding for technology designers and producers. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems.

Measures to improve **platform security** include:

Transport Layer Protection. The most common options available are Virtual Private Networks (VPN) or Transport Layer Security (TLS) model.

Prevention and Detection of SQL Injection.

Access Right Management System and Relevant Policies.

Authentication. The traditional form of security tokens like username/password are prone to phishing attacks and hence do not provide complete security. Instead iCROSS will use **Two Factor Authentication (2FA)**, adding an extra layer of security that is known as "multi factor authentication". Users are required not only a password and username (single-factor authentication) but two out of three types of credentials before being able to access an account.

Auditing. Auditing is the security concept in which privileged and critical business transactions are logged. At a bare minimum, audit fields that include who (user or process) did what, where (file or table) and when (created or modified

²⁶ Going beyond the secure storage and communication of data, Privacy Enhancing Technologies (PETs) now exist with counterintuitive capabilities such as anonymous communication across the public Internet; electronic cash that mirrors the anonymous nature of money in the physical world; and anonymous credentials that prove an individual has permission to access specific resources without revealing their identity.

timestamp) along with a before and after snapshot of the information that was changed must be logged for all administrative or critical transactions as defined by the business.

System Documentation. Documenting system components, networks, services, and software should provide for a bird's-eye view needed to thoroughly cover and consider security concerns, attack vectors and possible security domain bridging points. Just as with hardware, all software components should be documented, since this can assist in understanding total system impact due to a compromise or vulnerability of a specific class of software. A network topology should be provided with highlights specifically calling out the data flows and bridging points between the security domains.

Configuration Management. Configuration management allows avoiding the many pitfalls inherent in building, managing, and maintaining complex infrastructures. Tools will always be used to automate configuration and deployment. It is important that network devices, operating system, database, firewalls as well as software configurations are monitored on regular basis to ensure that their configuration is not changed by any unauthorized user.

Patch Management. Patch management is to manage the implementation of fixes in order to resolve the defects/problems identified.

Methods to improve **data protection** include:

Sanitisation of tenant data when program ends;

Encryption to protect sensitive information in transit and storage. For data in transit end-to-end encryption should be applied. It must be ensured that personal data in transit is protected against active (e.g. replays, traffic injection) and passive attacks (e.g. eavesdropping), thus ensuring data integrity²⁷.

The encryption keys should not be used by, or be accessible to anyone others than the border agency and the cloud service provider.

Storage encryption adds an additional layer of protection that will continue protecting the data even if an attacker subverts the database access control layer.

Backup is the most important means to keep the data from being lost due to intentional or unintentional access. It is also important to encrypt the up-to-date backups. Backup is easiest and the most familiar process for most situations

Data destruction, by effectively deleting personal data from disks and other storage media. Measures include immediate overwriting with random data²⁸, destroying/demagnetising the storage media, physically destroying the media so that it can no longer be used, usage of secure deletion software.

Interface with Social media

Border control processes today include the consideration were applicable of publicly available information. Such information may be that conference agendas and published papers for example of travellers to a scientific conference, similarly for athletes travelling to an athletic event, or representatives of merchants attending an expo, news and other. Social platforms can also shed light on travellers' affiliations and interests that will in turn guide some of the interview questions. iCROSS will develop search tool to perform preliminary search on public information and social media analytics to consult about the validity of the information at the pre-arrival stage, i.e. To check matching photo of the person with the name and nationality, etc. It will be developed in synergies with other research projects, especially IO-FACT on Digital Forensic Investigations and RUBICON on planning of border check processes, where partners participate or adoption of publicly available open source tools and will interface with iCROSS RBAT.

Integrated Border Control Analytics Tool (BCAT)

The underlying technical approach for the implementation of the BCAT is based on the utilization of all results produced by all the tools implemented in the project to perform post processing analyses in order to achieve two goals:

- Evaluate the performance of the each proposed task and compared its effectiveness to the human border control agent.
- Discover key patterns in the data associated with either False accept or false rejects of travellers based on the data collected in the Pilot study (but also applicable in the event of wide adoption of the iCROSS platform)

The analyses tools will be broken up into two categories, (a) the statistical analyses and modelling tools, and (b) the data mining-computational intelligence tools. The statistical analyses and modelling tools will reveal complex statistical models that will attempt to utilize the results of each implemented tool to improve on the system's overall effectiveness.

The data mining – computational intelligence tools will be targeted towards the identification of novel patterns in the intermediate, or final results of all the analyses tools applied to travellers that are associated with specific classes of travellers, for example travellers that are falsely accepted, or falsely rejected by human border control

²⁷ Integrity may be defined as the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission.

²⁸ Special software tools that overwrite data multiple times in accordance with a recognized specification should be used.

agents or by specific automated tools. Dimensionality reduction algorithms will be implemented to help identify which automated tool's results, or intermediary results do not contribute significantly to the final outcome of a traveller's accept or rejection decision for border control while feature selection algorithms will be implemented to identify the specific intermediary or final results of tools that tend to be strongly associated with the outcome of border controls of travellers. Various clustering approaches (hard, fuzzy, hierarchical) will be investigated to enable unsupervised identification of groups of travellers that share common characteristics in their collected data (honest/lying to the same questions, similar document authenticity results etc) as a method of identifying specific cases where either the human agents, or the proposed automated tools tend to consistently fail.

Furthermore, experimental workflows will be defined, sequences of analytic steps to be applied at regular intervals to provide descriptive statistics as to the performance of the iCROSS platform and the human border control agents. As an example consider performing document authentication first, and using the output of that analyses to guide the Avatar on asking questions related to his/her identity or how he/she was issued those documents.

Risk Based Assessment Tool (RBAT)

The RBAT module will act as an "automated decision-maker" on the data extracted during the iCROSS procedure. It will support the decision-making process of the application backend towards the end-users of the application (in this case the border-agents), while providing all the necessary measures to ensure that the appropriate information reaches the relevant group of users. This module can be developed on the basis of an ED existing tool.

More particularly, a complete point and click graphical environment allows authoring rules through the use of structured, non-technical expression of logical interactions between the "Business/Target User Objects". The administrator will have the capability in a very simple manner, which will not require prior knowledge of difficult programming languages, to author the appropriate conditions/rules in order to determine, according to the European/international laws, national regulations, "trends/tendencies" of the particular time-period, etc., the security level during the border check process and the risk-threshold that will classify accordingly the traveller and the customised procedure he/she will have to go through.

Some highlights of the RBAT module are:

- *User defined Criteria*
 - Easy, human-friendly and efficient compilation of logic involved
 - Completely User-Defined, loosely coupled with proprietary in-house IT Systems
 - Adaptable to new requirements or amendments
 - Natural language oriented Rule Based System and /or Algorithmic while the combination of both is supported
- *Rules.* A rule allows users to perform complex queries with specific criteria combining available data. The RBAT module is based on a full version control system that is explicitly bound to the decision making process. The complete history of the classifications made at a point in time is stored along with the rules that were used to arrive at each conclusion and all relevant data. The administrator is responsible for the maintenance of the rules that s/he created. The system provides a number of actions over the rules, such as add, edit, delete, copy allowing the performance of any desired adjustment.
- *Scoring schema.* RBAT provides scoring schema based on user-defined scoring mechanism. The user can assign a scoring value to each rule which depended on the type of the operator that performed in the evaluation process, i.e. exact match, contained, phonetic match. The scoring schema is tuned by the administrator of the system. *Definition of the scoring schema* is an entire research effort that will take place in collaboration with the end users and requires thorough validation to ensure that the risks are correctly assigned based on the data that result in their calculation. Several parameters contribute to the estimation of risk: the origin of risk parameter indicating whether it is coming from a reliable source as opposed to on publicly available data, the reliability of the source indicating whether it is based on reliable data and calculation or fuzzy methods (i.e. the INTERPOL list of criminal is a reliable source as opposed to an article listing criminals in a news web site), the degree of uncertainty in the calculation (the FMT gives more certain result than the ADDS), etc.

Hidden Human Detection Technology (HHD tool)

This tool has been suggested to solve an existing problem that is reported at the border control. In many cases the illegal travellers hide themselves in busses, cars or trains, since they don't possess the necessary travel documents. The authorities have to detect them and they do so, without appropriate tools to support them. This is the case highlighted in the pictures below. The portable HHD is proposed to facilitate this work.

As a secondary target, iCROSS will attempt to provide detection of people crossing land borders hidden inside vehicles or trucks and trains containers or open cargo wagons. The land border staff has often confronted "peculiar" situations with people hiding literally inside car seats, small closets or even suitcases. However, relevant checks are not performed routinely, especially when traffic flow across the check points increases; instead they are made occasionally or indicatively, unless dictated by official warnings, relying mostly on visual inspection and staff's

experience and perception. Thus, a need for portable devices is revealed, especially when more advanced equipment requiring large installations (i.e. x-rays for trucks and containers) is considered too expensive.

To this respect, iCROSS proposal aims at providing a portable radar prototype for the detection of hidden people, exploiting the Doppler frequency shift in E/M waves caused by breath or slight movements. iCROSS Hidden Humans

Detection (HHD) tool, lies upon a life detector CW radar for detecting trapped alive humans under building ruins, already developed by ICCS²⁹; an early version of which has already been tested in Athens earthquake (1999) assisting rescue teams, while three lab prototypes have been achieved in the meantime (one of them is tri-band in P, S and X-band). However, the situation in land borders concerning hidden humans is quite different than alive persons under collapsed buildings.

Although the basic concept remains more or less the same, several advances are in order to meet iCROSS needs. In the foreseen scenarios, the HHD tool will be carried and operated by customs officers or border staff. Thus, the range towards the “target” is smaller; resulting in compact portable module without loss of performance, with lower

transmitted power and smaller batteries. Based on the existing experience, frequencies of operation will be thoroughly investigated. As it seems, the lower microwave band (2.5 & 1.15GHz) is the best candidate for the relevant cases, combined with slot-type antennas instead of large horns. Other solutions will be also explored (i.e. UWB) while P/UHF and X-band will be sustained for flexibility and increased detection probability. In order to finally decide performance parameters, dual or tri-band modes will be used combined with alternative implementations and through measurements and testing in

both real and simulated cases for advanced performance.

Apart from open air use (vehicles and passengers trains or open wagons), for penetration through metallic containers or closed compartments, attempts of combination and data fusion with acoustic sensors (using sound echo signal) will be made (B version), based on quite recent advances³⁰ in high-power acoustic sensors technology. Sound penetrates metallic walls; thus, the acoustic sensor is an excellent complement to the radar one, due to its sensitivity to small and slow motions, allowing detection of stationary persons by breathing motion alone. Moreover, FFT and digital signal processing will be made locally with the use of smartphone or tablet, that will act as a CPU and, with a mobile-type app, enabling data local visualization and transmission to the iCROSS platform. On successful detection, the user will experience a beep alarm signal, triggering an in-depth inspection at a secondary level.

Therefore, HHD module will consist of two main units (sensors and tablet) resulting in a portable device complying to the iCROSS concept. Attractive features are also targeted: high-resolution, near-real-time data processing and display, low development cost and user-friendliness. In terms of the overall iCROSS platform and the TRL5 approach, the HHD tool is considered as a module to test and prove the technology, the integration ability and the applicability of operation and will be tested in vehicles and in the passengers / cargo train pilot

Wireless Technologies for Border Check Process

The wireless technologies requirement was imposed by the fact that at border checking the new technologies require specific Quality of Service (QoS) at border crossing station, within trains, or busses that is not guaranteed given their remote or mobile nature. This state-of-the-art technology supports this requirement.

The iCROSS project aims at speeding up and facilitating the land border control operations in automated manner. Travellers control envisages a two stages border check process including the pre-arrival registration and the reduced time actual control at the border, the implementation of which cannot exist without highly reliable, available, efficient and secure wireless communication systems. In order to provide a reliable, secure and user-friendly environment for the users, the wireless technologies that will be employed should meet specific needs and requirements: high-availability even in remote/rural areas, mobility requirement focusing on improved system performance in high speed scenarios and of course reliability and safety requirements.

The radio link availability depends primarily on the radio coverage of the wireless network that could be a cellular or a satellite system. Obviously, in case of the on-board check (and potential pre-arrival registration) scenarios, the requirement of high-availability is a challenging task due to the complexity of the scenario's environment; if, for example, the users travel by train, their route may include bridges, tunnels and viaducts. Vehicle's high speed may prevent a datalink connection due to the extremely short interval for handovers between cellular nodes. Moreover, in many cases, the vehicles travel through rural areas where cellular coverage is inadequate.

²⁹ M. Bimpas, N. Paraskevopoulos, K. Nikellis, D. Economou and N. Uzunoglu “Development of a Three Band Radar System for detecting Trapped alive humans under building ruins”, Journal Progress In Electromagnetics Research, PIER 49, 161–188, 2004

³⁰ Franklin Felber “Demonstration of novel high-power acoustic through-the-wall sensor”, Proc. SPIE 9456, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement XIV, 945603 (May 14, 2015); doi:10.1117/12.2084056

A reliable, cost-effective and easily deployed solution that can be employed is the satellite communication. Particularly, using the Ka band satellite technologies, the border security personnel (customs officers, border agents) or travellers can connect with a reliable, high-speed satellite link to the internet and send the required digital information to the control border centre while they are on the move. In case of trains, the trajectories are constant, consequently, proactive fade mitigation techniques may be applied (adaptive coding and modulation, and diversity techniques) in order to increase the availability and the reliability of the system.

Scenarios of on border crossing points and potential On Board checks

As discussed in the previous sections, during the pre-arrival registration stage, the traveller provides initial digital information to the iCROSS platform. Then, in the border crossing point the actual border control takes place by the security agents. Depending on the technological capabilities of pedestrians or travellers inside vehicles (cars, buses, trains etc.) the following wireless connectivity scenarios are foreseen: In the *first basic scenario*, on the border crossing point, iCROSS foresees the wireless connection via the portable iCROSS unit, of the border officers conducting the security controls to the iCROSS platform. In parallel the registration of those travellers that did not have the ability to pre-register may also take place. The *second scenario*, which is potentially more advanced, is basically meant for the border agents when in trains; since, in many cases the border agents move on-board the train from one country border to the other and vice versa, conducting passport and security checks and then return back on the next train. However depending on the facilities available, iCROSS may also facilitate even traveller's "on-board" registration; the traveller can provide certain information *during* his travel and before actually reaches the border crossing point, although being close to it (i.e. an hour distance). The relevant facilities require an *a priori* internet connectivity and wireless access to the iCROSS platform, provide that this is available; i.e. by the traveller's mobile devices while quite many applications nowadays involve existing internet availability through Wi-Fi in buses, shuttles or trains.

The required capacity and internet connectivity will be achieved through agreements (SLAs) with either fixed, or mobile or satellite operators. The rest radio network will be fully designed by iCROSS team.



iCROSS impact Assessment

iCROSS's integrated estimation of deceptiveness and suspect behaviour will be compared with the established border control procedures. Data about today's procedures will be collected to derive metrics that will indicate improvement or not of the task, based on multivariable analysis, aiming at the overall improvement of the procedures. A comparative approach of the data collected before and during the pilots will take place to help with the evaluation of the performance of iCROSS. Specific metrics will be set such as % correctly classified as truthful or deceptive. Contingency tables can be used to identify bias (i.e. high accuracy with classifying one category, low with the other).

Implementation approach

The iCROSS implementation approach follows the well-known V-model approach, focusing on a top to down way for the architecture design and iterative validation with end users of intermediate prototypes. The figure below highlights the workflow all along the project.

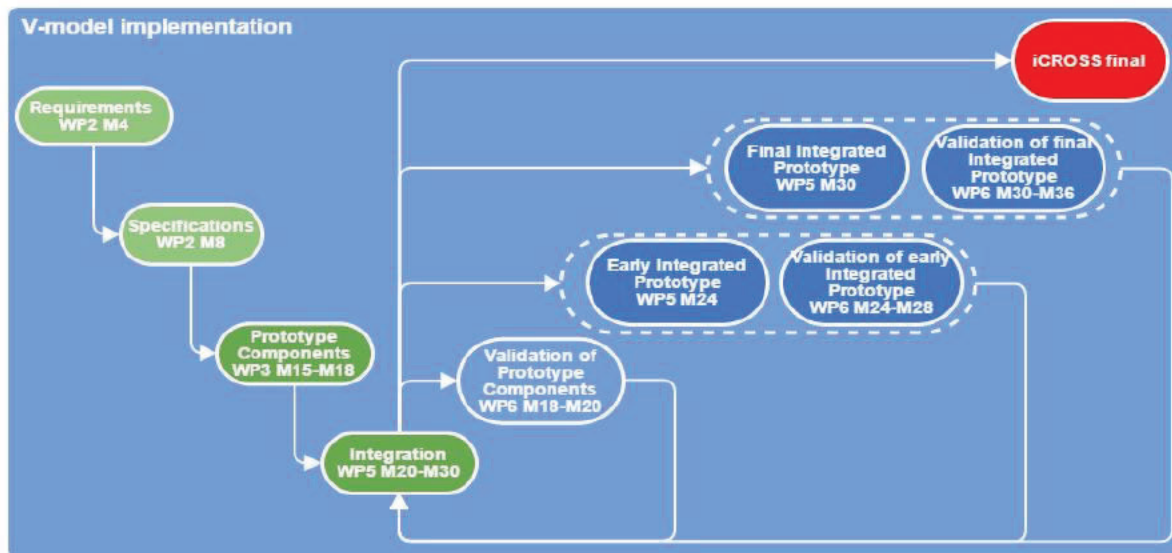


Fig 7: iCROSS V-model implementation approach

1.3.5. Sex/gender issues

With respect to the research topics addressed, the technology is essentially gender neutral. Regarding the consortium, it comprises of a well-balanced team with representatives of both genders, working together in an effective and productive way. Additionally the coordinator and technical manager are females but also leadership and relevant responsibilities are distributed to researchers of both genders. In that way, the iCROSS consortium promotes the successful collaboration of the two genders.

1.4 Ambition

User friendly mobile application for the traveller and the agent

As already presented in the technical approach, the focus of the ambition for the portable applications will be the user friendliness on the one side and the performance and speed on the other. This will enhance the efficiency of the operations at the border control. Novel techniques for designing user friendly interfaces will be designed

Document Authenticity Analytics Tool (DAAT) Ambition

FADO/PRADO created by ED for EC served as a European system for the exchange by computerized means information concerning genuine and false legal and travel documents and contained -among others- images of false and forged documents, images of genuine documents, summary information on forgery techniques as well as information on security techniques. Ever since many systems have been developed, including both software and hardware (hardware is fundamentally based on existing technology devices, e.g. IR/UV scanners, etc.), for document authentication, but their application is mostly “limited” to banks, casino groups, car-hire companies, etc. They have not yet adequately been utilized to support border control operations in real time.

iCROSS aims to overcome any ethical issues, sweep along the legal framework supporting the effectiveness of EU border control and apply these tools and knowhow and expand its purpose for the differing requirements and needs that arise for document processing in terms of their authenticity during border control operations by providing a full ICT customized and automated solution, in real-time and during the border control operations.

Automatic Deception Detection System (ADDS)

Biometrics

Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic such as: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data take an innovative step forward to **replace personal information (ID cards)** in order to ensure a faster and more secure and feasible verification of people’s identity. Biometric templates cannot be reverse-engineered to recreate personal information and neither cannot be stolen and used to access personal information. Using a unique, physical attribute

³¹ Sip Kamila Ewa, Carmel David, Marchant Jennifer L, Li Jian, Petrovic Predrag, Roepstorff Andreas, McGregor William B, Frith Christopher D: “When Pinocchio’s nose does not grow: Belief regarding lie detectability modulates production of deception.”, *Frontiers in Human Neuroscience*, Vol.7, 2013, No. 00016, p.1-11

URL=http://www.frontiersin.org/Journal/Abstract.aspx?s=537&name=human_neuroscience&ART_DOI=10.3389/fnhm.2013.00016

³² Joshua D. Meadors, Carolyn B. Murray: “Measuring Nonverbal Bias Through Body Language Responses to Stereotypes”, *Journal of Nonverbal Behaviour*, June 2014, Volume 38, Issue 2, pp 209-229, DOI 10.1007/s10919-013-0172-y

³³ Wojciechowski J, Stolarski M, Matthews G (2014) Emotional Intelligence and Mismatching Expressive and Verbal Messages: A Contribution to Detection of Deception. *PLoS ONE* 9(3): e92570. doi:10.1371/journal.pone.0092570

of your body, such as your fingerprint or iris, to effortlessly identify and verify that you are who you claim to be, is the best and easiest solution in the market today. Biometrics have been around for many years and recent modern advances in this innovative technology coupled with big reductions in cost makes it available and affordable to almost everyone: consumers, small business owner, larger corporations and public sector agencies.



Fig 8: Biometric symbol in e-passports

Nowadays, biometric information (i.e. fingerprints, palm vein data, iris recognition, etc.) is being incorporated in passports, known as **e-passports**. They are a combination of paper and electronic passport that contains the necessary information (included in an embedded RFID chip – effectively a contactless smartcard) to establish one's identity. To prevent wireless reading of the passport content without the owner's consent, passports can use a mechanism called Basic Access Control (BAC): to access the smartcard one must visually read some information printed in the passport. Subsequent communication between passport and reader is then encrypted to prevent eavesdropping. All EU passports implement BAC. However, it is expected that Supplemental Access Control (SAC) replaces BAC in the future due to the weaknesses detected among BAC. Other protection mechanisms are implemented in the contactless chip such as: (1) Passive Authentication, to detect any possible modifications of the chip and (2) Active Authentication, to prevent people from cloning the passport chip. Moreover, another protection mechanism is being implemented to protect fingerprints and palm vein data, which is: Extended Access Control (EAC). It simply consists in verifying that the chip and the terminal reader are not a falsification. All these features makes e-passports ideal, fast and secure for checking people's identity. The advantage of this technology is its fast extension within member states and therefore, most people already possess an e-passport. According to a report from Ryan Clary³⁴, the International Civil Aviation Organization (ICAO) reported that by 2011, 93 out of 193 United Nations (U.N.) member states, were issuing e-passports, with additional 21 countries ready to deploy the technology in the following years. The ICAO estimated that by July 2011, these 93 states had issued more than 345 million e-passports, of which at least 45 of them included fingerprints and 14 of them were planning to include fingerprints by the end of 2011. This report also mentions an IMS Research prediction of 90% e-passport domination by 2016. iCROSS is thus well positioned in time, since is now the time of implementing biometric verification systems at border controls.

Face Matching Tool (FMT) Ambition

Face recognition (FR) is by far the most convenient biometric means. Although face recognition has started to appear on many applications, especially under controllable environments, such as computer login, entrance and gaming devices, and has been piloted at several airports for checks and passport controls, there are still challenges to be addressed for a robust deployment. The biggest challenge comes under unconstrained environments where illumination variability and poor image quality are by far the most problematic issues for reliable applications in large-scale public services³⁵.

Ever since Turk and Pentland's seminal paper on eigenfaces³⁶, there have been tremendous progress in making face image based biometrics a practical tool. Worldwide laboratories and researchers have been competing to further advance the field with the notable methods such as, Fisherfaces³⁷, Features and Templates³⁸, Active Shape Model³⁹, Active Appearance Models⁴¹, Morphable Model⁴² and Local Binary Patterns⁴³. The Face Recognition Vendor Test (FRVT) 2006 is an independent evaluator for face recognition systems and largely represents the state-of-the-art performances with the best results achieving accuracy 99% under high resolution and controlled environment and 80% under unconstraint conditions, respectively. This provides a benchmark on FR system performances and indicates that reliability is expected between 80% and 99%. In order to enhance the system performance to the upper bound, natural variations (e.g. aging⁴⁴ ⁴⁵, expression, limited pose) and environment factors (e.g. lighting, ambient) must be addressed and integrated into the recognition models.

³⁴ <http://www.secureidnews.com/news-item/e-passports-spread-to-half-the-globe/>

³⁵ N. Firth, "Face recognition technology fails to find UK rioters", p.19, 20 August 2011, New Scientist.

³⁶ M. Turk and A. Pentland, "Eigenfaces for recognition," J. of Cognitive Neuroscience, vol. 3, pp. 71-86, 1991.

³⁷ P.N. Belhumeur, J.P. Hespanha, D.J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 19, pp. 711-720, 1997.

³⁸ R. Brunelli, T. Poggio, "Face recognition: Features versus templates," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 15, pp. 1042-1052, 1993.

³⁹ T.F. Cootes, C.J. Taylor, D.H. Cooper, J. Graham, "Active shape models-their training and application," Computer Vision and Image Understanding, vol. 61, pp. 38-59, 1995.

⁴⁰ A. Lanitis, C.J. Taylor and T.F. Cootes. Automatic Interpretation and Coding of Face Images, Using Flexible Models. IEEE Transactions of Pattern Analysis and Machine Intelligence, Special Issue in Face and Gesture Recognition Vol 19, no 7, pp 743-756, 1997.

⁴¹ T.F. Cootes, G.J. Edwards and C.J. Taylor: "Active appearance models. IEEE Trans. on Pattern Analysis and Machine Intelligence, 23(6), pp 2001, 681-685.

⁴² V. Blanz and Th. Vetter, "A morphable model for the synthesis of 3D faces," SIGGRAPH'99, pp.187-194, 1999.

⁴³ T. Ojala, M. Pietikäinen and T. Mäenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 24, pp. 971-987, 2002.

⁴⁴ A. Lanitis, C.J. Taylor and T.F. Cootes. "Toward Automatic Simulation of Aging Effects on Face Images". IEEE Transactions of Pattern Analysis and Machine Intelligence, Vol 24, no 4, pp 442-455, 2002.

⁴⁵ G. Panis, A. Lanitis, N. Tsapatsoulis, T.F. Cootes, Overview of research on facial ageing using the FG-NET ageing database. IET Biometrics, 2015

Various approaches addressing these variations and discrepancies in facial images appear in literature, among them, manifolds or dimensionality reduction methods are making great impact. The dimensionality reduction (DR) process and effect has been linked with the Deep Neural Networks⁴⁶, which has become a de facto architecture for solving complex cognitive tasks. They can be used to model and capture nonlinear variations among facial and lighting changes. Various DR methods and manifolds have been derived recently, Kernel PCA, Local Linear Embedding (LLE), ISOMAP, Laplacian eigenmap, Locality Preserving Projection (LLP), Self-Organising Map (SOM) and ViSOM, and their performances in aiding the FR have been evaluated⁴⁷ and results show that certain adaptive neural methods can make significant improvement on the performance. When further coupled with the efficient LBP and gradient based methods, they can boost the performance under unconstrained conditions to within 2-3% of the upper bound⁴⁸.

In iCROSS FMT will enable seamless interaction with both the traveller mobile device hardware that will be in the pre-arrival as well as the body mounted camera at the human agent interview

The integrated Border Control Analytics Tool (BCAT)

The BCAT tool will be implemented enabling combinatorial analyses using statistical modelling and data mining approaches of all available data. During the pilot phase of the project, this will enable the support of the real time analytic algorithms by enabling the integrated analyses of their final or intermediate results. However, the biggest value of this tool will be the ability to use novel approaches to re-analyse using the Pilot case data collectively:

- 1: The performance of each individual tool will be calculated by univariate analyses tools. Through this the validity, sensitivity and specificity of each tool will be compared against the human border control agent performing the task.
2. Any potential interaction effects between the results of multiple tools (subjects found to be marginally deceitful on question 1 and have marginal similarity with the picture on their travel documents, are strongly associated with travellers using invalid documents that human agents fail to identify correctly)
3. High (to include) or low (to exclude) performing automation tasks that contribute greatly to the final decision making support of the status of a traveller. These analyses will be implemented through data mining techniques such as feature selection and dimensionality reduction.
4. Finally, automated pattern discovery will enable the automated discovery of key patterns in the data of travellers matching the same outcomes. This could include intermediary results of analyses from some tools, and will have the advantage of helping discover new patterns. In this regard iCROSS envisages advancement of clustering approaches (particularly fuzzy) and distributed association rules to be of value in identifying relationships within the data.

HHD tool: Hidden Humans / Illicit Goods Detection in Land Borders

The detection of hidden humans and illicit goods in borders security, is a challenging whole project by itself, incorporating extensive multidisciplinary research; technology for the easy fast and effective detection of humans hidden in a variety of vehicles (cars, trucks, containers, trains etc.) is still not available to customs and border guard services. Current commercial solutions mainly involve high energy x-rays detectors; however, in land borders the whole vehicle, truck or cargo container should be subject to x-rays and large commercial vendors⁴⁹ offer integrated systems finding hidden contraband through more than a foot of steel. However, such technology solutions are either too expensive or difficult to deploy in all border control scenarios, requiring demanding installations which reduce applicability especially for extended border lines.

⁴⁶ G.E. Hinton and R.R. Salakhutdinov. "Reducing the dimensionality of data with neural networks," Science, vol. 313.5786, pp. 504-507, 2006.

⁴⁷ H. Yin and W. Huang, "Adaptive nonlinear manifolds and their applications to pattern recognition," Information Sciences, vol. 180, pp. 2649-2662, 2010.

W. Huang and H. Yin, "On nonlinear dimensionality reduction for face recognition," Image and Vision Computing, vol. 30, pp. 355-366, 2012.

⁴⁸ W. Huang and H. Yin, "Binary gradient correlation pattern for robust facial representation," submitted to IEEE Trans. On Pattern Analysis and Machine Intelligence, 2014.

⁴⁹ Rapiscan Systems <http://www.rapiscansystems.com/>, SmithsDetection Inc. <http://www.smithsdetection.com/>, Leidos Inc.

Although for illicit goods, mostly explosives, portable or desktop trace detectors exist commercially, this is not the case for hidden humans; profiling and detection dogs have proven to be the most effective. Moreover, for rising cross-border flows with high throughput, time is limited for in-depth controls, therefore vehicles and containers are not systematically checked. FP7 Security Calls addressed the issue while the following solutions can be highlighted among the Security Research projects⁵⁰: artificial sniffers based on human perspirations/CO₂ (SNOOPY), olfactory sniffers (HANDHOLD, SNIFFER) with bio-mimicry biosensors and linear ion trap mass spectrometry, Terahertz technology - THz (TERASCREEN). Other technologies include heartbeat detectors, mm-waves, laser distance measurement, telescopic inspection mirrors/cameras, EM field detection and chemicals.

In past years, several researchers suggested Non-ionizing EM radiation using CW Doppler radar as Life Detector of trapped persons within collapsed buildings, through their breath or slight movements^{51,52}; penetration depth and spatial resolution are the main trade-offs for iron loaded concrete. Quite recently, similar concept's NASA/JPL's Finder module⁵³ helped saving lives in Nepal earthquake (April 2015). Nowadays, the relevant interest has increased for patients' vital signs contactless monitoring, and for high security requirements i.e. see-through-wall radar, airport and entrance security monitoring, border patrol etc. Although in the 1980s, relevant microwave systems focused at the X-band (10 GHz), it turned out that it cannot penetrate difficult material. Other systems at UHF (450 MHz) and at lower microwaves are better, with 2.5GHz and 1150 MHz⁵⁴ penetrating easier metallic wire mesh concrete. More recent advances use UWB pulses radars⁵⁵ showing high penetration capability, immunity against multipath interference and large bandwidth for better separation between target and clutter.

Millimetre (mm-) wave passive and active imaging offers rapid remote detection of metallic and non-metallic objects and contraband concealed beneath clothing⁵⁶, enabling "through-the-wall imaging systems (TWIS)" and humans' remote observation for military and law enforcement personnel, but not through metal walls. Passive mm-wave (PMMW) radars are much better for outdoor detection of concealed weapons in human body⁵⁷, while THz technology⁵⁸ is also an emerging candidate for concealed non-metallic weaponry. Multifrequency microwave radars⁵⁹ detect human movements and gestures through micro-Doppler signals, at short (S-Band, through-wall, up to 3m) or long ranges (W-Band, mm-waves, up to 100m in free space) through wideband noise or continuous single tone.

iCROSS HHD tool aims at a simple, portable solution, exploiting already gained knowledge on the field through ICCS's legacy life detector module. Although in natural disasters timing and exact location is everything for the survival and rescue of victims, this is not the case herein. Increased accuracy in location or in-depth screening are not absolutely targeted in iCROSS scenarios; but rather a small-range alert tool, enabling the use of electromagnetism coupled with newest achievements in acoustic sensors (sound echo) for tracking people also behind metal walls. EM waves cannot penetrate metallic structures and this is a real challenge especially for the cargo containers scenario; however, these are not EM shielded and leakage through their walls or doors may reach a highly sensitive receiver. Higher frequencies (X-band) show excellent spatial accuracy of detecting very slight movements (i.e. breath acquired in front of a human) but penetration depth is limited and vice versa; lower frequencies (VHF/UHF bands) have much higher penetration depth but can detect only large motions (i.e. an intensive hand movement). Thus, acoustics sensors are better solution for the metal walls case.

Summarizing, the iCROSS HHD radar aims to further advance the humans' detection technology when hidden in vehicles/closed compartments with portable, easy to use, contactless and reliable characteristics, tailored to the land borders security staff everyday procedures and working activities. Considering that the final outcome will be an advanced lab prototype, the aim is to contribute as possible to the iCROSS overall concept for effective portable devices. Above all, to prove that such modules could be successfully integrated in holistic systems of broader applications and to pave the way for potential integration of other similar research or commercial devices in the future (i.e. illicit good detectors that could also be optional for the open iCROSS platform).

⁵⁰ Work Programme 2013 Cooperation Theme 10 SECURITY, <http://cordis.europa.eu/search/result>

⁵¹ Chen, et al., "An X-band M/W life-detection system" IEEE Trans. Biomedical Eng., Vol. BME-33,697–701, July 1986.

⁵² Aggelopoulos, Karabetos, Constantinou and Uzunoglu, "Mobile microwave sensor for detection of trapped human beings" Journal of Int. Measurement Confeder., Vol. 18, No. 3, 177–183, July 1996

⁵³ Article: <http://www.jpl.nasa.gov/news/news.php?feature=4578>, Media Contact, E. Landau, NASA's Jet Propulsion Laboratory, Pasadena, CA.

⁵⁴ Changzhi Li, et al, "Radar Remote Monitoring of Vital Signs", IEEE Microwave magazine, February 2009, pp 47-56

⁵⁵ Ossberger et al, "Non-invasive respiratory movement detection and monitoring of hidden humans using UWB pulse radar", Joint Intern. Conf. on UWBST & IWUWBS. 2004

⁵⁶ G. Richard Huguenin, "Millimeter-wave concealed weapons detection and through-the-wall imaging systems" Proceedings of SPIE - The International Society for Optical Engineering 1997 (1997).

⁵⁷ Xiang et al, "Development of passive mm-wave imaging for concealed weapon detection indoors" Microwave and Optical Technology Letters Volume 56, Issue 7, pages 1701–1706, July 2014 (2014).

⁵⁸ Tribe Kemp et al, "Hidden object detection security applications of THz technology", THz and GHz Electronics and Photonics III, Proc. of SPIE, Vol. 5354 (SPIE, Bellingham, WA, 2004) pp 168-176

⁵⁹ Narayanan, et al, "A Multifrequency Radar System for Detecting Humans and Characterizing Human Activities for Short-Range Through-Wall and Long-Range Foliage Penetration Applications" International Journal of Microwave Science and Technology Volume 2014 (2014).

Radio Communication Networks

The iCROSS project aims at exploiting wireless and satellite communication technologies to speed up and facilitate the land border control operations in an automated manner. Nevertheless under the framework there will be some important advances in the field of wireless and satellite communication technologies in various aspects such as physical layer and channel modelling, cooperative and relaying techniques, in radio resources management techniques and spatial distribution and connectivity evaluation.

1. *Physical layer advancements in Wireless and Satellite Communication Technologies*

Description of operations at the pilot sites

A. Hungarian Border

The external Schengen border in Hungary is about 1139 km long, consisting of border sections to: Croatia (EU), Serbia, Romania (EU) and Ukraine. Currently, with a 175 km section in the main migration route, the border between Hungary and Serbia can be considered as a hotspot. Protected by a 4 m high fence enhanced with NATO barbed wire, temporarily set up along the green border on the Hungarian side, it is not only interesting because of push of the

⁶⁰ A. D. Panagopoulos et al., "Satellite Communications at Ku, Ka and V bands, Propagation Impairments and Mitigation Techniques", IEEE Communication Surveys and Tutorials, 3rd Quarter, pp.1-13, October 2004.

⁶¹ K. P. Liolis, et al., "On the Combination of Tropospheric and Local Environment Propagation Effects for Mobile Satellite Systems above 10 GHz", IEEE Transactions on Vehicular Technology, Volume: 59, issue: 3, pages: 1109-1120, March 2010.

⁶² P. D. Arapoglou, et al., "Railway Satellite Channel at Ku Band and Above: Composite Dynamic Modelling for the Design of Fade Mitigation Techniques", International Journal of Satellite Communications and Networking, Jan. 2012.

⁶³ K. P. Liolis, et al. "On the Applicability of MIMO Principle to 10-66GHz BFWA Networks Capacity Enhancement through Spatial Multiplexing and Interference Reduction through Selection Diversity", IEEE Transactions on Communications, vol.57, Issue 2, pp. 530-541, Feb 2009.

⁶⁴ V. K. Sakarellos, C. Kourogiorgas, A. D. Panagopoulos, "Cooperative Hybrid Land Mobile Satellite-Terrestrial Broadcasting Systems Outage Probability Evaluation and Accurate Simulation", Wireless Personal Communications, July 2014.

illegal migration,⁶⁵ but also facing a huge wave of passenger traffic. This direction is also the route of the Eastern-European and Asian workers employed in the EU and travelling home for holiday every year. This means a wave of traffic between mid-June and mid-September is huge at this border section, it can be up to 10 000 vehicles per day with an average of 3000 vehicles per day, usually each with families of 3-5 or larger groups (mini-, midi-, and large buses). This daily pressure counts up to ~580000 vehicles exiting and about the same number (~588000) entering the Schengen Area at this section.



B. TRAINOSE-Greek border

TRAINOSE will host a train border-check pilot case, using as test-field the Eidomeni (GR) – Gevgelija (MK) border stations. The above mentioned border stations were selected due to the initial passage from an EU member country (Greece) to an Non-EU / Non-Schengen member country (FYROM) and vice versa. For this demonstration, two different cases will be examined; one will deal with a passenger train, whereas the other will employ a freight train.

CASE A: Passenger

⁶⁵ Crossing the green border without permission is an offence in Hungary, therefore who commits it has no right to stay in the country, its presence is illegal.

⁶⁶ <http://www.cit-rail.org/>

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

In case of containerized cargo it is difficult for someone to get in the containers because they are sealed and it is easy for the controllers to spot a broken seal and perform a comprehensive check by opening it upon request of the authorities.

But in case of conventional cargo there are too many locations that can be used by individuals to cross the borders without them being spotted by the authorities.

In any case and if there are any sounds or evidences that someone moves on the train, then the police authority of the station take under the situation and proceed to checks and even request for opening the cargo units by the staff of the station.

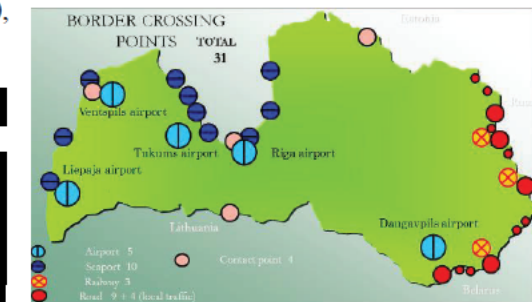
C. Borders of the Republic of Latvia

State Border Guard of the Republic of Latvia (SBG) is a direct administration State institution, under the supervision of the Ministry of the Interior. On issues of guarding and control of the State border, as well as on issues, which are associated with the control of the observance of the entry, residence, exit and transit of aliens and stateless persons regulations, and other issues within the competence.

Main tasks of the State Border Guard are Border checks of persons and means of transport at BCP, surveillance of the land and sea border between BCP, control of foreigners residence into the country and expulsion of illegal migrants (immigration control), investigation of criminal cases on illegal crossing of the state border and people illegal movement, identification of asylum seekers and documents' expertise.

Total border length of Latvia is 1878 km including land border - 1380 km and sea border - 498 km. Latvia has border with Estonia (EU) - 343 km, Lithuania (EU) – 588 km, Russia – 276 km and Belarus – 173 km.

There are totally 31 border crossing points (airport -5, seaport -10, railway -3, road -13)



departure

D. Polish borders

Poland has an external EU/Schengen land border of 1163.25 km with non-EU/Schengen countries (state borders with Russian Federation, Republic of Belarus and Ukraine) along with 418 km external EU/Schengen sea border. Specifically, the whole Polish borderline is about 3512 km long, consisting of 440 km sea border and 3072 km land border: 210 km with Russia, 104 km with Lithuania (EU), 418 km with Belarus, 535 km with Ukraine, 541 km with Slovakia (EU), 796 km with the Czech Republic (EU) and 467 km with Germany (EU) as seen in the map below. Thus Poland is actually an EU external border and considering the presence of one main airport and 10 regionals in the country, the necessity to improve tools and methods in the context of automated border control systems, esp. with



Source: study of Border Management of Headquarters of Polish Border Guard

PBG - Polish Border Guard is the main Polish organization for the conductance of border checks and traffic control, and the protection against illegal immigration

Border Guard Regional Unit	Check Points			Border crossing points					
	Overall	External	Internal	Totally	Land	Railway	River	Sea	Air
	93	60	17	72	19	14	1	13	20
Warmińsko-Mazurski Regional Unit	11	10	1	3	4	3	—	—	1
Podlaski Regional Unit	18	13	3	9	4	4	1	—	—
Nadbużański Regional Unit	20	20	—	12	7	4	—	—	1
Bieszczadzki Regional Unit	14	14	—	9	4	3	—	—	2
Morski Regional Unit	8	9	—	21	—	—	—	13	3
Nadwileński Regional Unit	6	5	—	6	—	—	—	—	6
Śląsko-Małopolski Regional Unit	7	2	5	2	—	—	—	—	2
Nadodrzański Regional Unit	11	3	8	6	—	—	—	—	5

Source: Border Management of Headquarters of Polish Border Guard

Section 2. Impact

2.1 Expected impacts

Expected impacts listed in the workprogramme

Expected impact list from the call	Expected impact – iCROSS
..lead to novel mobility concepts for land border security	iCROSS expected impact has the potential to become the fifth tier added to the access control model of the Integrated Border Management: in addition to embassies, Schengen cooperation, border control and measures within territory (in-depth checks), benevolent frequent travellers will begin to contribute to the effectiveness of the Schengen System, providing advance passenger information (API) on their free will, forecast traffic and generate feedback. Furthermore, iCROSS elevates the land border security with several new concepts, technologies and procedures that aim to improve speed and increase accuracy and reliability. A combination of novel and existing technologies will be integrated into a coherent and user driven system to ensure that the requirements of future land border control are met and proofs are provided. The integrated analytics tools that provide novel insights and intelligence and contribute in novel ways in identifying threats and vulnerabilities will contribute to frame the way risk scores are allocated as components for better planning and decision making for the border operations as well as for future predictive analytics across real-time border transactional data, better situational awareness and more targeted intervention.
enabling authorities to achieve higher throughput at the crossing points whilst guaranteeing high security level	With the use of the pre-arrival checks, average processing time is expected to drop by one third per traveller and authorities will be able to focus on risky passenger categories and individuals, achieving a higher security level. Furthermore, with increasing numbers of people and vehicles crossing borders every year there exists a strong demand for new ways of performing biometric recognition whereby throughput is increased, security is maintained or increased and all processing is performed in a legally and ethically compliant manner. Therefore iCROSS provides significant potential to deploy advanced technologies and analytics to enable border guards to perform enhanced risk assessment as for example, to detect attempts to evade identity checks, or choosing a particular moment to enter the border zone because the traveller believes that when increased numbers of travellers are passing through the identity checks will be less thorough. These tools collect information and enable border conformance checks and reporting and the detection of anomalous behaviour, focusing on optimization of traveller flow.
Enabling fast processing of passengers within vehicles or pedestrians	iCROSS expectation is, that average processing time of a third country national will drop by at least 30%. According to the recommendation of the Schengen Evaluation Committee, the average time for a thorough check shall be around 3 minutes, while a minimum check is 45 seconds. We are aiming at shrinking the time of the thorough check to the duration of minimum check, but taking into consideration, that not everybody will register and the penetration of internet connection and mobile devices is at low rate in certain countries, we set a reachable target with aiming at a least 30% drop in average (including non-registered travellers). This drop will result from the decrease in the number of steps the border guard has to carry out manually during thorough check. According to the Schengen Border Code, travel document validity (holder identity, expiration, date of issue), visa (if required), purpose and means of stay, existence of an alert on refusing of entry has to be checked and the traveller shall not pose a threat to public health, public security or international relations of the MS. The detailed list for HNP border guards, how to carry out these checks consist of 17 elements. With the use of iCROSS, only part of document validity (including identification of holder) has to be checked at the first line, the rest will be already assessed by iCROSS and results will be provided for the border guard. So time taken for thorough check of a low-risk third country national will take no more time than a minimum check for an EU citizen without relaxing border checks meaning level of security will be maintained continuously.
improving the efficiency of passengers flow management	Using the statistical module of the system and risk-based approach that deploys effective scanning and inspection technologies, border crossing points can be informed of expected numbers of travellers in advance, as travellers complete their pre-arrival check on the platform. Furthermore the portable units can detect and prevent illicit crossings of people and goods. Previously this was mainly available at airports and harbours; with iCROSS concept it can become a reality at road BCPs in wider extent.

<p>Harmonization of requirements across Member States and Associated Countries (and standardization) is expected to also automatically greatly improve affordability</p>	<p>iCROSS is an effort to establish common procedures and assessment criteria and mutual approaches for identifying, classifying and addressing risks at the land borders. It is an approach that includes 4 EU member states end users (3 of them governmental authorities) that will define, develop and evaluate integrated start-to-end procedures and rules.</p> <p>The iCROSS analytics tool in addition to the risk based approach is expected to contribute to collaboration and coordination across border controls and enhance the SIS, EES and RTP with more information from land border not so far considered. Agreed and common risk model and standardized types of information collected and specified processes can improve communication between them. This is the beginning of an era where LEA can exchange information about travellers and goods, to organize public and private stakeholders to activities that can strengthen security and efficiency.</p> <p>Standardizing procedures and data not only save effort, by sharing and exchanging important information, but also generate savings resulting from streamlining and stimulating border security operations. With standardised procedures vertical, national implementations that increase costs can be replaced to achieve economies of scale. iCROSS contributes a step towards a more integrated and harmonised border control in EU area. An added bonus to this effort in standardization is the fact that it would ease the integration of new technologies and procedures across all the member states and associated countries reducing the costs of including innovative solutions to border control. Development of integrated mobile system for border control concept, will use the experiences with the operational work of the Border Guard in different EU countries. The acquired competence in this area, along with the knowledge obtained during the iCROSS project work will help to define the recommendations hardware and design of system to meet the requirements set for full functionality useful in the performance of duties by Border Guard officers. Providing connectivity for the mobile border control system with national databases connected to VIS, SIS II, EES will allow for immediate verification of a person crossing the border. This will increase the reliability of border control work carried out in the field and improve the procedures for the elimination of risk of penetration into the EU of unauthorized persons, or who use someone else's identity.</p>
--	--

Meeting Needs of European and global markets

According to the World Tourism Organization⁶⁷, the number of international arrivals shows a growth from a mere 25 million international arrivals in 1950, to 806 million in 2005, to a staggering 1.087 billion in 2013. The Organization forecasts a further growth in international tourist arrivals of between 4% and 4.5% in 2015 and by 2030; they expect the number of **people crossing international borders to exceed 1.8 billion per year**, which will undoubtedly increase the strain on border control.

Enabling smooth and fast border crossing for travellers, while ensuring an adequate level of security, is a challenge for many Member States. Currently, the Schengen Borders Code requires a thorough check at entry of all travellers crossing the external border; the system is largely depending on the human agent and its ability to capture the deceptive and illegal behaviour. The same checks are applied to all third country nationals, regardless of the level of risk associated with them or their frequency of travel. Although there are already measures and tools available at EU border crossing points, such as the Schengen Information System (SIS)⁶⁸ and Visa Information System (VIS), none is comprehensive enough and tackle the entire procedure from start-to-end, to ensure appropriate border crossings within the EU territory. The SIS is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area, in particular to carry out checks on persons who may have been involved in a serious crime or may not have the right to enter or stay in the EU. The main purpose of the VIS is to allow the verification of a traveller's visa application history and, at entry level, verify whether the person presenting the visa at the border is the same person to whom the visa has been issued. None of them can consult in real time about suspects that are not yet listed. From the above it gets clear that the border control operations and their security lies in the centre of the Europe's political agenda as indicated by already existing and complementary European initiative (Smart Border Initiative).

Additionally, the European Commission has proposed the allocation of €3.5 billion from the €4.7 billion Internal Security Fund 2014–2020 to external borders and visas, including large-scale IT systems. The priorities for the fund are “The further development of an integrated border management system by improving, replacing, and upgrading

⁶⁷ <http://mkt.unwto.org/en/barometer>

⁶⁸ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm

equipment/infrastructure for visa and borders according to new technological developments. This would in particular include enhancing the operational capabilities of the member states within the framework of EUROSUR standards.”⁶⁹ Furthermore, in July 2010, in “The Global ePassport and eVisa Industry Report”⁷⁰, it was projected that ePassports become mainstream and significant penetration has been achieved; therefore the next logical step would be the proliferation of ABC solutions. In 2014, the ABC eGates began to gain significant traction in the global marketplace. In another report by Acuity, it was estimated that for Airport, Land Border and Sea Port, the overall systems’ deployment were counted to be 75,000 units worldwide (both fully automated as well as partially automated), which proves a still limited market size that will certainly be further developed.

According to EU statistics⁷¹ “In 2013, around 325 000 non-EU citizens were refused entry at the external borders of the EU28. More than 70 % of these cases were recorded in Spain (192 775) and Poland (40 385). In 2013, 12.4 % of the total number of EU-28 refusals were recorded by Poland, due largely to the high number of entry refusals (97 %) from Russia, Ukraine, Georgia, Belarus, Armenia. The preliminary check on entry and stay requirements will be able to significantly decrease this number by informing travellers on lack of entry and stay conditions (meaning a refusal) in advance. With checking travel document, visa, means and purposes as well as the SIS II alert on refusing entry, taking the same year, 119 195 travellers would have been informed in advance, meaning 36% less refusals, thus less administration work and staff effort for border guards.

	2008		2009		2010		2011		2012		2013	
	Refusals	%	Refusals	%	Refusals	%	Refusals	%	Refusals	%	Refusals	%
EU-28	634 975		499 640		394 800		343 005		316 015		324 840	
Belgium	1 170	0	2 055	0	1 855	0	2 730	1	2 390	1	1 535	0
Bulgaria	4 060	1	3 030	1	3 070	1	2 810	1	3 070	1	2 550	1
Czech Republic	255	0	380	0	330	0	360	0	190	0	310	0
Denmark	70	0	60	0	80	0	115	0	95	0	140	0
Germany	7 215	1	2 980	1	3 550	1	3 365	1	3 820	1	3 845	1
Estonia	2 325	0	915	0	1 665	0	2 205	1	1 915	1	1 400	0
Ireland	5 260	1	3 560	1	2 790	1	2 545	1	2 205	1	1 935	1
Greece	2 055	0	3 000	1	3 805	1	11 160	3	9 415	3	6 995	2
Spain	510 010	80	387 015	77	290 045	73	227 655	66	199 830	63	192 775	59
France	16 695	3	14 280	3	9 840	2	11 100	3	11 310	4	11 745	4
Croatia (*)											10 015	3
Italy	6 405	1	3 700	1	4 215	1	8 635	3	7 350	2	7 370	2
Cyprus	895	0	670	0	685	0	575	0	545	0	430	0
Latvia	875	0	670	0	815	0	1 230	0	1 820	1	2 050	1
Lithuania	2 210	0	1 750	0	1 965	0	2 215	1	2 215	1	2 865	1
Luxembourg	5	0	0	0			0	0	5	0	0	0
Hungary	5 530	1	7 700	2	10 475	3	11 790	3	9 240	3	11 055	3
Malta	120	0	140	0	130	0	80	0	200	0	300	0
Netherlands	3 160	0	2 500	1	2 935	1	3 500	1	2 515	1	1 990	1
Austria	2 715	0	645	0	400	0	445	0	245	0	360	0
Poland	16 850	3	26 890	5	23 015	6	20 225	6	29 705	9	40 385	12
Portugal	3 600	1	2 565	1	2 060	1	1 795	1	1 240	0	810	0
Romania	8 920	1	4 595	1	4 750	1	3 620	1	3 340	1	3 410	1
Slovenia	7 565	1	7 895	2	7 845	2	7 970	2	7 665	2	4 780	1
Slovakia	1 540	0	855	0	840	0	595	0	595	0	435	0
Finland	1 775	0	1 300	0	1 185	0	1 420	0	1 640	1	1 735	1
Sweden	55	0	35	0	90	0	155	0	155	0	180	0
United Kingdom	23 640	4	20 460	4	16 365	4	14 720	4	13 300	4	13 435	4

Fig 9: Non-EU citizens refused entry at external borders, by EU Member State⁷²

In the Hungarian border it is estimated an average checking time for persons enjoying the right of free movement and stay (EU families) is no more than 10-15 seconds per person, and up to 3 minutes for checking third country citizens. The estimated average of 3.5 million persons crossing the border every year and estimated third country citizen rate is 48% (~1.7 million). According to official statistics the last five years averagely 32 million foreigners crossed the Hungarian borders every year. Annual total passenger flow for Schengen borders is estimated between 490-585 million border crossings per year.

The challenge of iCROSS is to bridge and complement the market needs, the efforts and initiatives of the EU and provide additional IT tools to improve the planned services in EU and globally wide.

Target Markets and Size

As iCROSS challenges are valid for all European and Schengen Territories border control authorities, these constitute the target market, but also territories beyond Europe can be addressed by partners. Indicators of the investments and interest is evidenced by the following:

Automated Border Control (ABC) solutions are fundamentally transforming the global travel experience. From Australia’s SmartGates and US Global Entry to the hundreds of eChannel gates at Hong Kong land and sea crossings, to the Automated Passport Control Kiosks rolling out across North America, and the nearly 200 eGates planned for deployment in the UK and Germany next year, ABC technology is driving the development of the 21st century international transportation infrastructure.

⁶⁹ “Borderline, The EU’s New Border Surveillance Initiatives”, A study by the Heinrich Böll Foundation, June 2012

⁷⁰ <http://www.acuity-mi.com/index.php>

⁷¹ http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_enforcement_of_immigration_legislation

⁷² http://ec.europa.eu/eurostat/statisticsexplained/index.php/File:NonEU_citizens_refused_entry_at_external_borders_by_EU_Member_State_2008%E2%80%932013_V1_1.png

According to a market report⁷³, published by Transparency Market Research, the global homeland security market was valued at USD 245.72 billion in 2013, growing at a CAGR of 5.6% from 2014 to 2020 to account for USD 364.44 billion in 2020.

The major factor driving the growth of homeland security market is several government initiatives undertaken to restrict increasing terrorist threats and cross border insurgency. In addition, rising cases of illegal immigration, drug smuggling and human trafficking are compelling the governments of various countries to invest heavily in procurement of homeland security products.

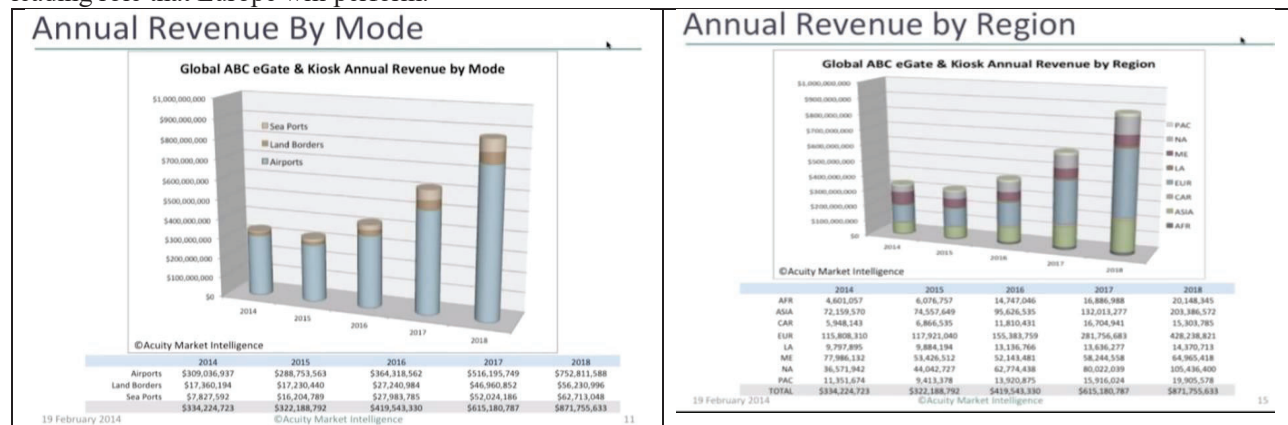
More particularly, and as far as Automated Border Control (ABC) is concerned, Acuity Market Intelligence reports⁷⁴ that the rapidly evolving ABC eGate and kiosk market will generate more than \$1.2 billion dollars in annual revenue by 2020. The total number of ABC eGates deployed as fully automated replacements for border control stations is projected to exceed 6,000 by 2020. An additional 33,000 specialized immigration self-service kiosks and eGates will be deployed at check-in, baggage drop, arrival halls, and boarding gates at airports, land borders, and seaports worldwide.

Nearly 50% of the total number of eGates deployed at all airports, seaports and land borders are in Asia. Europe leads in airport deployments with nearly 40% of global units. eGates are estimated to increasingly be used at land borders; today they just represent 4.7% of all eGates deployed.

Europe will be the largest market for ABC eGates and kiosks representing a 47% total revenue market share from 2014 to 2020. Asia will follow with 22.5% revenue market share over the forecast period.

Airports are, for the time-being, the dominant sector in the ABC eGate and kiosk marketplace, nevertheless by 2020, they will cede ground to land borders and seaports.

Indicative numbers are presented in the following figures, clearly showing the increase in land border needs and the leading role that Europe will perform.



Other impact (Environmental, social, etc.)

Efficient border control operations has a variety of **social impacts** primarily in ensuring that borders remain under surveillance and are controlled.

Border Management is a challenge but comes together with a great opportunity since it will help contribute towards **an increased amount of security for all citizens** with more **secure borders**.

This supports tourist activity, and also helps to ensure safety for all by:

- Reducing the number of illegal immigrants who enter country borders undetected
- Increasing internal security as a whole by contributing to the prevention of cross border crime
- Increasing internal security as a whole by contributing to the prevention of cross border terrorism
- Reducing the traffic of drugs, weapons and illicit substances
- Preventing deaths of illegal immigrants entering countries

Barriers to achieving the expected impact

A number of persistent barriers can be identified, which the project's design has considered and should be overcome:

- Initial Investment:** The investment needed to research, design, implement and commercialize a tool like this will discourage most stakeholders. iCROSS is meant to be a foundation stone where they can build upon.
- Procedures and Technology reform:** The adoption of iCROSS implies important reframing and adjustments to border control processes and infrastructures as well as the daily work of border control authorities. Thus final adoption in everyday practice underlines central decisions, financial support, education and training, etc., which the nations have to adopt.

⁷³ <http://www.transparencymarketresearch.com/homeland-security-market.html>

⁷⁴ http://www.acuity-mi.com/ABCair_Report.php

- iii. **Critical mass of End users and Policy regulators:** iCROSS is integrating and improving psychological factors research and technological tools of diverse nature to improve border control operations. Due to its nature, the future adoption is only guaranteed with a critical mass of policy regulators, end users and stakeholders, which adopt and participate in the initiative and promote it further.

2.2 Measures to maximise impact

a. Dissemination and exploitation of results

The iCROSS dissemination & exploitation strategy in line with the innovation management approach consists of several policies, intended for the transfer of project achievements and lessons learnt and mainly to commercialise project results. The planning of dissemination policies, which is a *horizontal* procedure along the overall project lifecycle, will start immediately with the start of the project. In general, dissemination & exploitation policies will be based on the following:

Dissemination to European Industry	<p>The industrial partners and public bodies will disseminate the usage of iCROSS within their companies and organisations, out of the department or unit in charge of iCROSS participation and through their networks. Dissemination will be produced by means of the following mechanisms:</p> <ul style="list-style-type: none"> • Informal knowledge dissemination within each organisation, through internal websites or newsletters. • Meetings of iCROSS related staff with other personnel out of the project (in order to identify synergies). • Dissemination to related Business Interest Group (BIG) - the following indicative potential target groups for dissemination of non-confidential information iCROSS vision and innovations are initially identified: <ul style="list-style-type: none"> ○ Border control/face recognition technology tools/Sensors/Document recognition hardware and services suppliers (Business domain): iCROSS will share non-confidential information about the potential and the progress of the project for potential translation to other fields of interest, further exploitation of the results. ○ ICT applications suppliers and Industrial Community (Technological domain): iCROSS frontend and backend environment in terms of software and cloud-based applications/platforms and their technology will be demonstrated together with its publicly available documentation so that it can easily be the basis for many other applications for other target groups and even other application domains. Partner [REDACTED] are active in the provision of IT and commercial solutions in the private and public sector in sensors/tools/data integration and other domains and will disseminate the project results to their channels.
Dissemination to the scientific community	<p>The iCROSS consortium is strongly motivated for providing technological and scientific results that will be of major importance and interest for the scientific and industry communities. These results will be communicated in iCROSS website, at scientific, ICT and Security society meetings, submitted for publications in peer-reviewed journals and in press releases for popular and sectorial magazines, and newspapers. Efforts will be made to promote Open Access policies.</p> <p>In addition, the Scientific Council of the Hungarian National Police intends to host scientific and press events to present the project to the public, as follows:</p> <ul style="list-style-type: none"> ▪ 3-day national workshop for border guard, legal, technical and human rights experts in Hungarian, to generate significant input for relevant WPs; ▪ 3-day international workshop for experts to elaborate relevant findings in WP6; ▪ 2-day national conference to present results in Hungarian; ▪ 2-day international conference to present results of the project, inviting Central and East Europe Border Guard and Police authorities, foreign representatives, the Frontex, the Borderpol, the Cefpol and the Europol, EU-LISA. <p>Prior to each event, a press release will be released by the police and press will be invited to the last day of the events where there will be a press event and the consortium will give interviews in Hungarian and in English. Conferences will be broadcasted live and also recorded. Presented papers will be published in a peer-reviewed publication with ISBN number in both (English and Hungarian) languages.</p>
Dissemination of Knowledge to the wider	<p>Many of the partners involved in the iCROSS project are heavily engaged in collaboration projects concerning Security and e-borders/e-customs on a national and international scale. These collaborations allow these partners to transfer knowledge, and also to extract new challenging problems that require research to achieve new knowledge. ED is a major provider of IT solutions and services in 27 countries for the public sector and will thus disseminate the project knowledge and results through its activities and partnerships. In [REDACTED] and</p>

	<p>The iCROSS project intensifies this mutual insemination. It is an invaluable advantage for the partners to be able to produce experience with collaboration that has led to excellent research results and at the same time produced significant commercial impact. Periodic plenary and thematic/work package meetings will be held and involve all relevant public and industry partners.</p>
Dissemination to policy makers and reform	<p>iCROSS results will be disseminated to policy makers to the extent that this technology needs to be integrated in several border control facilities, aiming at the public sector. Thus information as illustrated in the sections below will be accessible to national policy makers. Private confidential meetings with European reimbursement agencies, European regulatory offices or notified bodies will be organized whenever requested, for advices and recommendations for the development of iCROSS intelligent border security system.</p> <p>The Hungarian National Police intends to bring results to European and national stakeholders with presenting results at 1) the Frontex Management Board, 2) Annual International Border Guard Conference 3) to Borderpol (an international NGO of border guards around the globe).</p>
Commercial exploitation	<p>Recognized by iCROSS consortium as the key driver for any future commercial success. The commercial exploitation plan is always based on a study that shall deal with the Background and Foreground Rights, the Patents, trademarks and IPR issues, which will be in the base of the future iCROSS product, taking account of EU policies, including those to foster the transfer of technology to SMEs, and promoting the use of generic, non-proprietary technologies, as well as the overall European security framework. In order to design a successful Exploitation strategy, the exploitation document will be developed taking as a reference the <i>Business Model Generation</i> (proposed by "Osterwalder&Pigneur" in 2010).</p>
Educational use	<p>As the research/academic/public authorities institutions engaged in the iCROSS project have teaching duties, the results of the project will place them in a position, where new alleys in the education of students or trainees can be exploited. The results of the iCROSS project will be used to provide students/trainees, research fellows and several companies with teaching and consultation services. These services will entail the transfer of knowledge and know-how to interested entities in the fields of: biometrics, sensors, IT platforms/databases, data fusion, and borders security.</p>

Path towards commercialization

Dissemination and exploitation efforts and materials are to be generated and their viability, integrity, complementarity, and consistency are supervised in WP7. iCROSS exploitation and commercialisation depends upon:

- Privacy regulations which are based on international and European regulations but may vary in each country, and thus require to be addressed in order to be commercialisable and ensure its wider acceptability and use.
- The modernisation of working processes and workers' management procedures, equipment and software that facilitates border monitoring and security and support of the facility management of the public sector authorities and the promotion of this plan within the public workers.

A stepwise approach to ensuring maximal exploitation of project results will be pursued:

Step 0: Understanding the full value chain and building the value creation, and the business /use case early in the project which will be achieved in line with the project's innovation approach.

Step 1: Investigation of all relevant market segments and further potential application areas, including legal, financial issues, competition and business planning taking into account of marketing studies and socio-economic research and carrying out complementary primary research where required. This activity will be mainly performed by marketing departments of iCROSS industry partners, in order to understand the possible threats and defining the proper wordings to be used in internal product leaflet in order to respond to the regulations in Europe and rest of the World.

Step 2: Analysis of complementary and competitor services and equipment in the market and wider community; identification of emerging best practice across the border security management internationally.

Step 3: Develop the deployment and business scenarios, market and business models for individual exploitation and joint exploitation, specifying collaboration roles, costs and revenue flows thus enabling calculation of net return over time for each type of market player, commercial and/or public; Identification of exploitation paths including the product roadmap, certification accreditation, commercial licence, etc. This will involve the socio-economic analysis of the solution and its impact.

Step 4: Organisation, planning and execution of wide impact dissemination activities to create full awareness of iCROSS activities and approach in the academic community, the Security, the ICT and general RTD community.

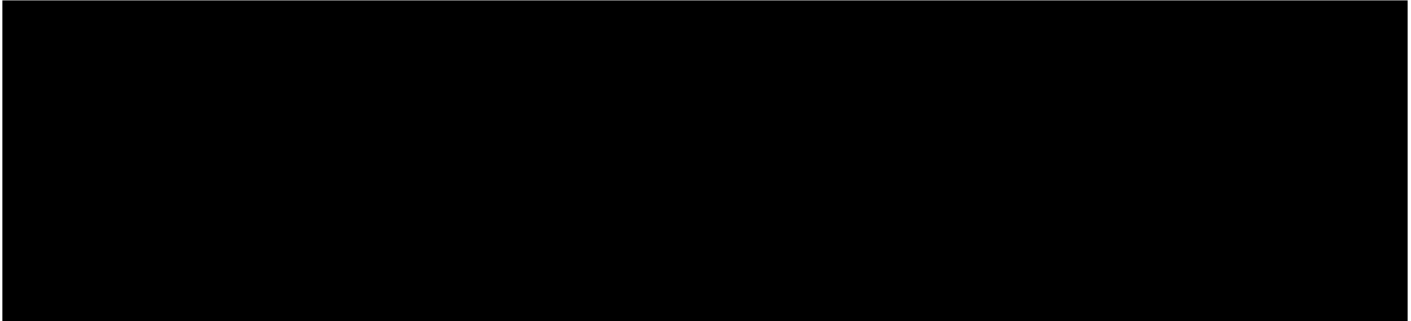
Step 5: Regular review, revision and refinement of partner-specific exploitation plans and joint/collaborative business plans in the light of interim project results; formalisation of service level and other appropriate agreements for joint exploitation among partners and third parties including possible creation of new legal entities (joint venture).

Step 6: Development and publication of a short evidence document outlining the experience and results of deploying iCROSS in real life scenarios, to be used for convincing new adopters of iCROSS solutions.

In general, if the project is successfully completed, it is expected that sufficient interest may have been raised from the market to enable initialisation of commercialisation procedures. However, commercialisation will require small additional investment and will not take very long after the completion of the project. The following key standards will be though foreseen to comply with during and after the project commercialisation:

Early joint exploitation plan

iCROSS consortium covers the whole supply chain as explained in the figure below:



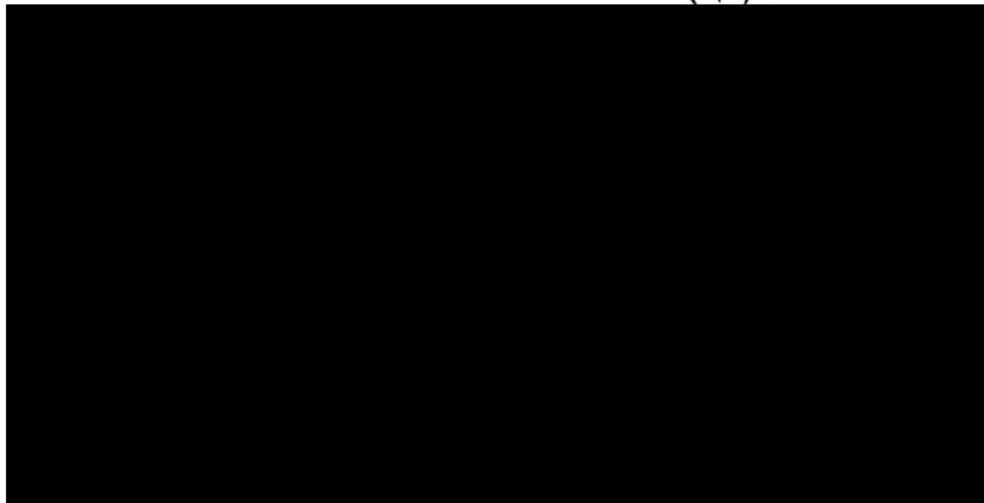
The consortium intends to commercialize the outcomes of the project through **alliance agreements** with the partners led by ED, a well-established and respected corporation in the ICT market with multiple successful products and services on the market

. This alliance exploitation agreement will outline the commercial cooperation roles-responsibilities and costs-revenues among the partners which developed system components and will be developed at the middle of the project when more is known about the exploitation plans.

An alternate method of capitalization on the iCROSS project's outcome for all its members is by exploiting the expertise they will gain in border control automation. Currently due to the limitations associated with border control (closed environment, classified procedures, hard to acquire realistic data) specific research is difficult to perform and the unique blend of consortium partners in this project will enable everybody to benefit from the added expertise, and network expansion that will be maintained through the established iCROSS alliance.

Exploitable results

The exploitable results are the entire platform but also the partial results of the individual tools and scientific research that will be the result of iCROSS. The following figure outline the main results, the exploitation paths and the partners interested in each of them.



Commercialisation model

iCROSS is a fully scalable system that is by design inter-operable and based on a scalable architecture; thus can be easily deployed in all EU countries' points of external entry. iCROSS platform with its mobile units and novel concepts for land crossing will be commercialised as a whole as well as partially by:

- Protecting the IPR of the relevant consortium partners for specific tools found to be successfully deployed and meeting expectations through the Pilot study making it available through a licensing scheme to border control authorities

- Developing the iCROSS platform and its tools can be offered to public authorities by answering to specific tenders by partners led by [REDACTED] and in alliances to offer the complete or partial solutions as required in each case. The platform will be offered in terms of license costs in addition to services to install, customize the tools and train the end users in the various countries. [REDACTED]
- Providing consultancy services that will built upon the expertise of the partners and the iCROSS experience.

Individual exploitation & use plans

ED is a leading innovative IT company, acting internationally, which is always interested to enlarge its current activities. ED has proven in its long history that it can successfully launch new products and services in the international market, and this is proven by the number and the importance of its clients (see profile).

[REDACTED]

ICCS is a very active non-profit, Academic, Research Institute, addressing multi-disciplinary fields, being at the forefront of knowledge-intensive competitiveness, representing the dynamic academic Greek sector.

[REDACTED]

STR Stremble Ventures is a research and development company focused heavily on further developing its portfolio of services and technologies. The core of STREMBLE is its multi-disciplinary team of scientists that come together to tackle challenging and often complicated tasks requiring inter-disciplinary expertise and cooperation.

[REDACTED]

[REDACTED]

MMU

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

ITT

[REDACTED]

EVR is a multinational group born in Spain with a commercial network around the world that provides global solutions for critical systems in the fields of Aeronautics, Space, Defense, Security and Emergency, based on engineering developments and innovative technologies developed both in-house and by third parties. EVERIS AD does provide the most leading technology, developed by ten Spanish companies which make up the group, taking advantage of the flexibility and speed in R&D and innovation processes.

Everis has a broad experience in working with biometric technology and [REDACTED]

[REDACTED]

BIOSEC is an R&D company specialized on developing biometric authentication solutions based on palm vein recognition especially in the field of IT security, mass identification and access control. BioSec's major goal is to further widen the portfolio of services and products through system integrations with third party systems.

[REDACTED]

JAS is dynamically growing technology company, operating in telecommunication, IT and national security. The company's strategy involves continuous development in the implementation of new products, technologies and processes.

LUH

HNP, PBG, TRA, BS

IPR Strategy

IPR management is crucial when developing complex software as it requires certainty as to the property of IP and a perfect understanding of the features, consequences and effects of the licenses accepted and/or used. Key developers and managers need explicit rules on how to access pre-existing know-how and foreground knowledge and qualitative and practical information support on how to ensure the protection of intellectual property as well as the ability to address legal issues with licensing experts.

The IPR management strategy will be the responsibility of the Project's Steering Committee and will be explicitly supported in the Consortium Agreement. It will include:

- raising participants awareness regarding IP issues
- contributing to the resolution of disagreements between participants
- assisting in the drafting of the plan for the use and dissemination of foreground
- tracking down results that should be protected and advice the individual partners on the means of protection
- assisting the participants in evaluating their contribution to the jointly owned foreground and establishing their respective shares
- deciding regarding third parties joining the consortium with the intention to receive the ownership of the Foreground of a specific Party.

The Project's steering committee will consist of one representative of each Party. The Coordinator will chair all meetings of the Project's steering committee. Decisions will be taken by a majority of two-thirds (2/3) of the votes. Each Member of a Consortium Body present or represented in the meeting will have one vote.

All IP management issues will be documented in the Yearly Exploitation and Dissemination Reports. There, it will be included a formalization of service level and other appropriate agreements (including IP agreements and conditions e.g. fair, reasonable and favourable conditions) for joint exploitation among partners and third parties, including possible creation of new legal entities (joint venture).

The iCROSS Consortium Agreement will be developed and signed **before the kick-off** of the project **taking into account the following preliminary agreements:**

- [REDACTED]

Open access

One of the expected means to disseminate the project results will be scientific publication. Such publication will be decided in conformity with the intellectual property, confidentiality and publication provisions set out in the consortium agreement. The destination will be selected once the co-authors have been authorized to publish by the project partners. It will be chosen among those which both respect the authors' interests and accept open access publication (with or without embargo period). The partners will use an open access repository, connected to the tools proposed by the European Commission (openAIRE, etc.), to grant access to the publications and to a bibliographic metadata in a standard format including information requested by the European Commission.

b. Communication activities

Target groups of the communication strategy

The communication planning will evolve together with the project's maturity phase. Moreover, the communication strategy is focusing on creating awareness and attracting potential future supporters of the project and its results. In the following table the phase plan, as well as the target groups are presented:

PHASE	Phase 1: Initial awareness phase (M1-M12)	Phase 2: Targeted awareness market phase (M13-M24)	Phase 3: Strategic phase (M25-36)
OBJECTIVES	<ul style="list-style-type: none"> • Agree upon Communication strategy and future activities • Create an initial awareness in the markets related with iCROSS project objectives and scope 	<ul style="list-style-type: none"> • Create a more "targeted awareness" regarding iCROSS technologies with key players and potential users • Inform about the technological benefits to 	<ul style="list-style-type: none"> • Maximize target market and industry awareness regarding iCROSS system by providing more tangible results, i.e. from pilot trials, verification and feedback from pilot users.

	<ul style="list-style-type: none"> • Present the concept, objectives and expected results 	the target market of iCROSS <ul style="list-style-type: none"> • Demonstrate early results (components and early technical validation results) 	<ul style="list-style-type: none"> • Demonstrate more advanced results (components and intermediate and final validation results)
ACTIVITIES	<ul style="list-style-type: none"> • iCROSS logo validation • iCROSS project web-site • Event, literature, research source identification • Press release • Project leaflet • Select events for attendance and start attending 	<ul style="list-style-type: none"> • Refine web-site with more concrete results and news • Social media and online promotion, such as news about early results in Twitter, Facebook, etc. and newsletter • Publish brochure, press release with intermediary results • Distribute marketing material • Attend events • Create YouTube videos showcasing components and intermediary results • Publish scientific papers in conference journals 	<ul style="list-style-type: none"> • Refine web-site with news, videos, photos, public deliverables and partial results • Social media and online promotion, such as about early results in Twitter, Facebook, etc. and newsletter • Publish brochure, press release and newsletter to registered parties and partners' relevant contacts • Distribute marketing material • Attend events • Workshops • Issue final press release • Create YouTube videos showcasing the system in trials and users' opinion • Publish scientific papers in conference journals • Demonstrations and feedback of trials evaluation
Target Groups			
Public workers and wider public	Funders and policy making bodies	Enterprise and Industry	
Public workers, facility managers, working conditions advisors, IT engineers, Students, Researchers and the general public	Policy makers in government, ministries and Regulators-Managers etc. Donors, Grants providers and Development partners, Representatives from international and national development cooperation agencies	Industry stakeholders, Private sector: Intelligent Border/Security suppliers companies, electronics and sensors manufacturers, mobile, web and IT developers.	

The project will aim at four levels of communication: awareness, understanding, action and participation. The target groups of each level have been identified and are presented in the table above. **Awareness** will mainly involve delivering the main message of the iCROSS project in relation to its aim and objectives, while **understanding** will require the providing of more detailed information on the project purposes, methods and deliverables. Involvement in both of these two stages will provide the basis for communication for **action**, where the project products will be delivered for further use. Communication of information is particularly necessary when targeting stakeholders likely to participate (in supporting the project), namely those who will offer financial, administrative and technical support within the project duration.

Efficient communication during the project will make use of a variety of dissemination tools. This will include:

Development of iCROSS visual identity

A **visual identity** will be developed for the project comprising a logo and style guidelines for on-line and off-line publications including at least the following applications:

- The project logo and website; Online banners; Social media accounts (project's online 'persona'); a Wikipedia entry; PowerPoint presentations; Exhibition stands; Project leaflet and other promotional material. A consistent look but also consistent written communication, a set of standard project descriptions and key messages will be provided.

iCROSS website and operation

An interactive and accessible project web site will be developed by ED and made available before *Month 1* of the project. The website will be referred to in all iCROSS public documents and presentations, as well as its QR code for easy reference. An easy and convenient content management will be provided making use of the open source content management software "Drupal". The public section of the iCROSS website will provide:

- a brief project summary in journalistic style highlighting the objectives, the contents and the structure of iCROSS
- a short profile of each partner and link to each site
- access to the project Public Deliverables and abstracts of selected non-Public Deliverables;
- publications and presentations at external conferences in various formats (pdf, MSWord, etc.);
- events section, promoting the events that the iCROSS consortium participates or (co-)organises.
- interactive features, such as questionnaires and/or FAQ, allowing for periodical online activation to be used for collecting end-users input whenever this is need, i.e. Towards the requirements analysis,
- visible links to the social media accounts of the project
- technical & scientific information (e.g. white papers) and user-oriented information;
- Relevant web sites of interest for the project such as companies, institutions, etc.
- Factsheets, reference materials and results produced within the project itself, including deliverables.
- Contact us section

A counter of visitors and other statistical tools will be used (including a visitors' feedback form), to monitor the usability and interest created by the web site and the project. The goal is to have a continuously increasing average number of web visits at monthly level.

The content of the website will be managed by: ED (general); the IP Management Team for the technical and scientific content.

Electronic newsletters

Short electronic newsletters, or e-newsletters and YouTube videos, informing key stakeholders of project developments will be developed

- The e-newsletter is issued on a six-month basis in English, so the frequency of publication must be maintained at all times whereby regular intervals are respected.
- The e-newsletter must be short.
- Each piece of news must be short, and concluded by a hyperlink that will invite the reader to get more information through the website.

The newsletter will include details of the project (Basic description of the project; description of the partners; description of the methodology and indicators), updates on its phases, a description of the preliminary technological enablers, summarization about the progress of the implementation of the specific technological enablers within the prototype, reports on the project's participations in events, proposed topics for the workshops, conclusions of the workshops, relevant media coverage, interviews and / or quotes from stakeholders' opinions regarding the necessity of the project, description of the final conclusions of the project;

Social media and online promotion

Facebook, Twitter and Google+ accounts will be set up for the project, with the aim to foster more accessible communication. YouTube channel will be set up, for easy upload of footage from the workshops, demo clips and other. The icons will be integrated in the website, for the audience to be aware of the availability for "conversation" of the project.

Publications and Participation in workshops, conferences and events

Participation of the project to up to 30 relevant European or international events (workshops, conferences and exhibitions) taking place within the European Union mainly (but not limited) to promote the project and its results. iCROSS events will be chosen taking into account the objectives set out in the project communication plan. Indicatively, a list is presented but will be further updated during the course of the project with more actual information. A detailed proposal for such events with the associated timing and objectives will be included in the communication plan to be presented on Month 6. The goal is to have at least 10 presentations and Demos in Conferences each project year. Key to the traditional dissemination strategy is to focus on a number of scientific and business publications outlining key technical achievements or business potential. The following provide indicative list:

<p>will specifically target the following journals:</p> <ul style="list-style-type: none"> ○ IEEE Intelligent Systems ○ Expert Systems With Applications ○ Computers & Technology ○ Information & Management ○ IEEE Transactions on Neural Networks and Learning Systems ○ International Journal of Neural Systems ○ Journal of Nonverbal Behaviour ○ ACM Transactions 	<p>and the following conferences:</p> <ul style="list-style-type: none"> ○ EASST – European Association for the Study of Science and Technology ○ EMAC - European Marketing Association Conference ○ ECIS - European Conference on Information Systems ○ International Conference on Information Fusion ○ EURO ID exhibition ○ World e-ID congress ○ SDW – Security Document World Exhibition ○ SMi Border Security Conference ○ IEEE International Conference on Artificial Neural Networks ○ IEEE World Congress on Computational Intelligence ○ Smart Borders Conference 2015 ○ European Day for Border Guards (FRONTEX)
---	--

In addition, some results of the project and announcements for iCROSS workshops and conferences will be disseminated through:

- Practitioner (trade) conferences such as ACI (Airports Council International), MMU have lots of experience with mass media – this contributes to acceptance by public
- Press releases and media interviews since i.e. MMU has a good track record in TV/radio interviews (whenever it is relevant);
- The websites of other thematically-related EU projects;

Preparation of publication and promotional material

iCROSS promotional video

A Promotional video will be prepared that will illustrate, in eloquent and business oriented style, the overall results of the iCROSS project and its success stories. This video will be promoted at the project web site, but also at YouTube. Leaflets and Posters Flyers: 2.000 copies, A4 recto verso, full colour, and posters: 200 copies, A1, full colour will be produced in two stages:

- By end of month 6, focusing on project objectives, challenges, and expected benefits for the project stakeholders, with aim to attract interest and involvement of stakeholders and SMEs in the pilot actions
- By end of month 20, focusing on project objectives, challenges, and results achieved, with aim to widely promote the project achievements and expected impact for customs and taxation across the EU and beyond.

The quantity for each material in each of the two phases will vary in function of the project needs and objectives, according to the expected distribution number which will be identified in the Communication Plan and limited by the maximum quantities proposed.

Participation in workshops, conferences and events

Participation of the project in up to 20 relevant European or international events (workshops, conferences and exhibitions) taking place within the European Union mainly (but not limited) to promote the project and its results. iCROSS events will be chosen taking into account the objectives set out in the project communication plan. Indicatively, a list is presented but will be further updated during the course of the project with more actual information. A detailed proposal for such events with the associated timing and objectives will be included in the dissemination plan to be presented. The goal is to have at least 10 presentations and Demos in Conferences each project year.

Collaboration with other projects – iCROSS will collaborate with other relevant projects aiming at exploiting synergies and impact increase. The envisaged fields of activity include joint activities for exchange, dissemination and training and coordination of standardisation efforts.

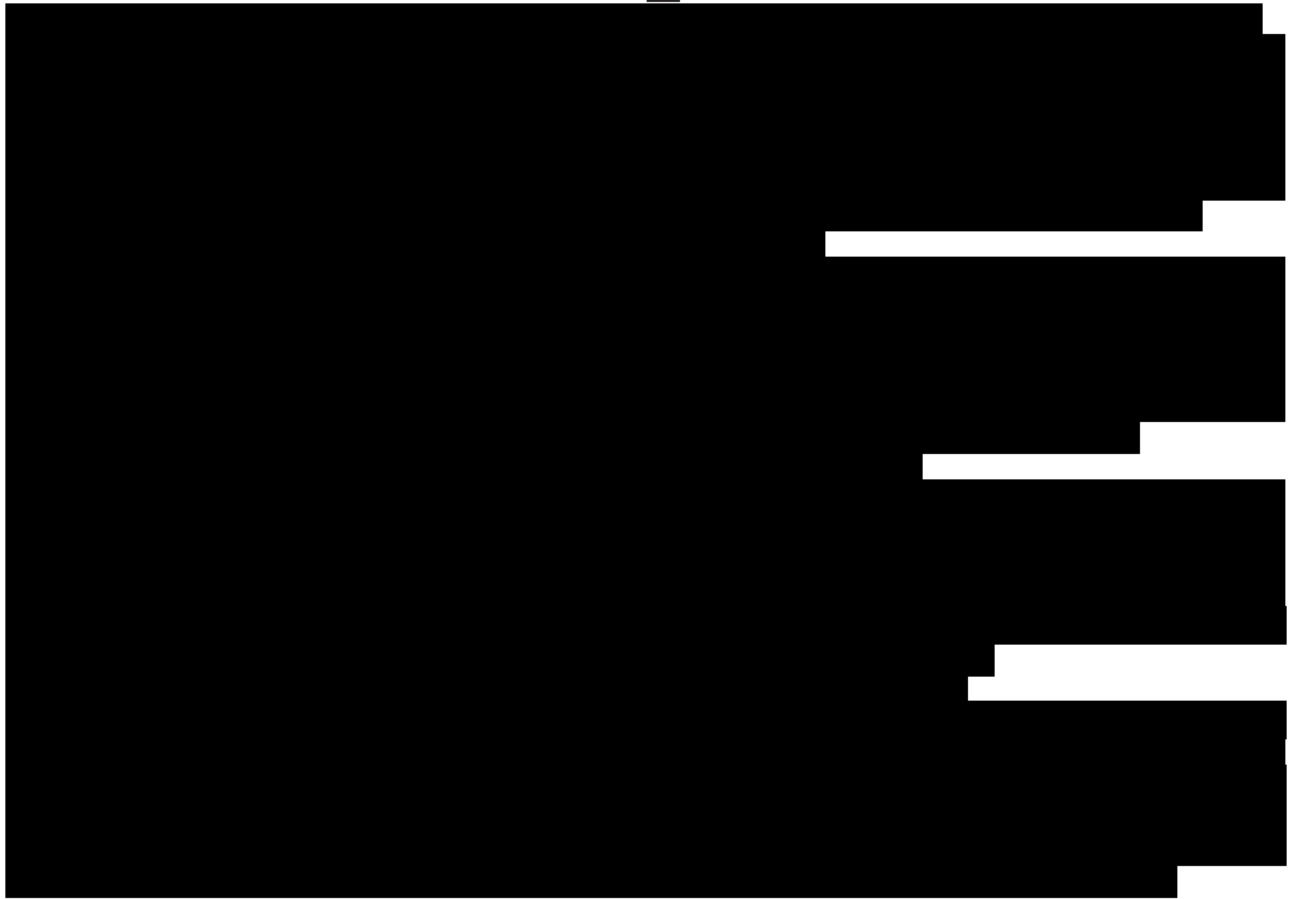
Section 3. Implementation

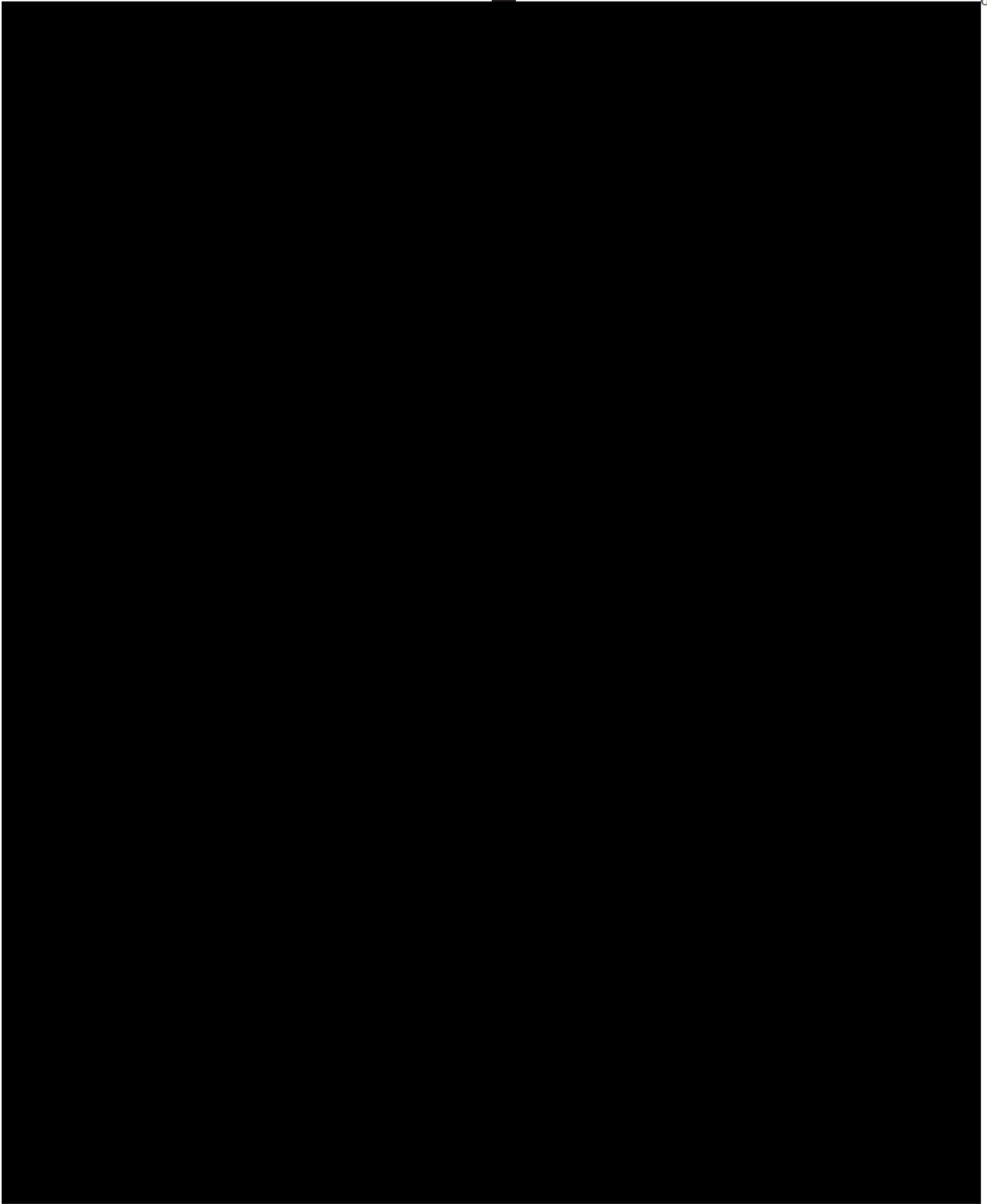
3.1 Work plan — Work packages, deliverables and milestones

[REDACTED]

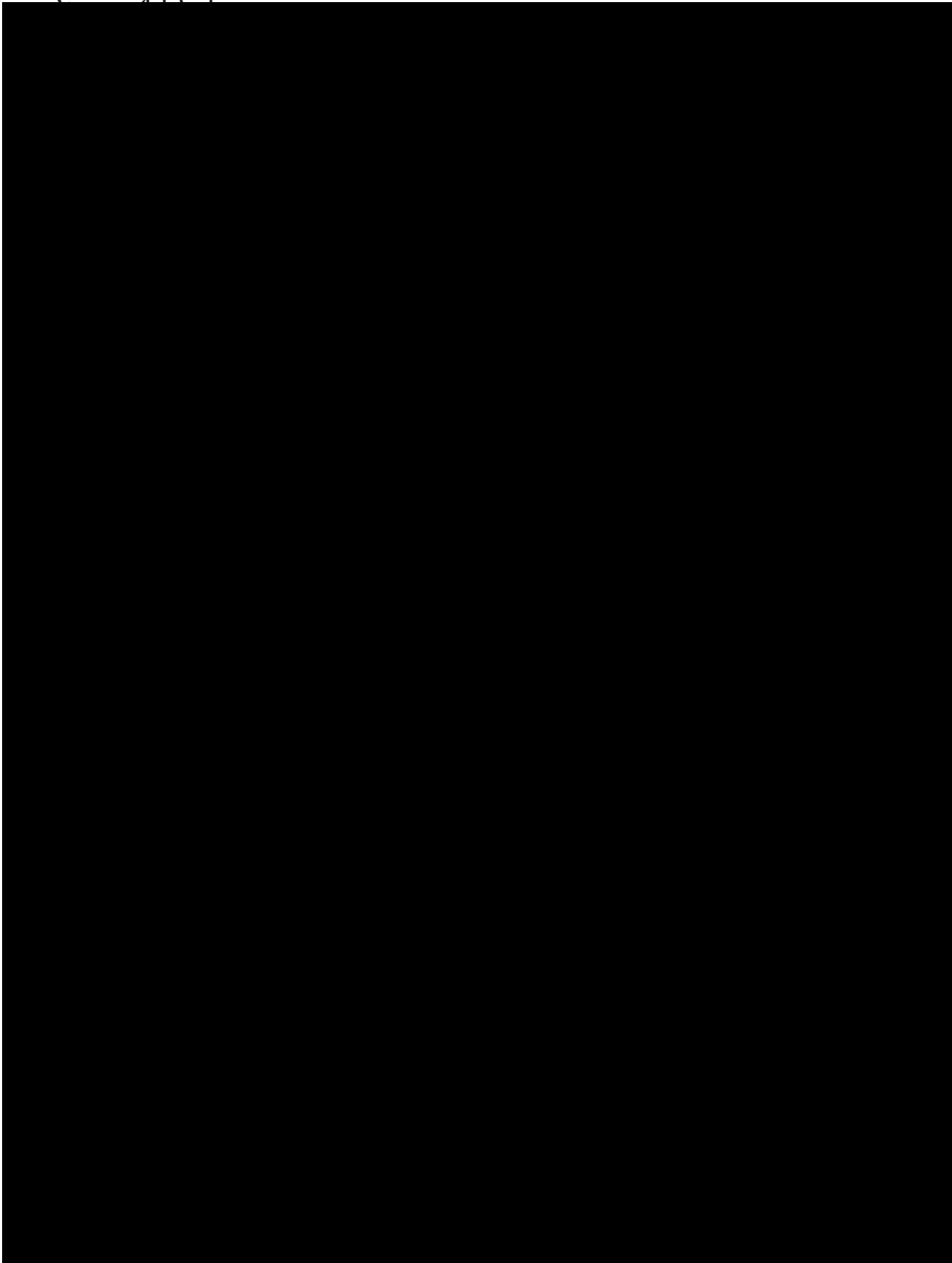
[REDACTED]

[REDACTED]





C a t c h



3.2 Management structure and procedures

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

Figure 1. A schematic diagram of the experimental design. The subjects were divided into two groups: the control group and the experimental group. The control group received a standard training program, while the experimental group received a modified training program. The subjects were then tested on a series of tasks, and their performance was compared between the two groups.

[REDACTED]

[illegible]

[illegible]

[illegible]

F

F **E** [REDACTED]

[illegible]

F **E** [REDACTED]

[illegible]


[700626] [iCROSS] – Part B

59

Section 4: Members of the consortium

4.1. Participants


1. European Dynamics Luxembourg SA

NAME:	 European Dynamics Luxembourg SA.				
Short Name:	ED	Country:	Luxembourg	Partner #:	1
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>EUROPEAN DYNAMICS SA (ED) is a leading European software vendor and Information and Communication Technologies (ICT) services provider, operating internationally through its offices and antennas in Alicante, Athens, Berlin, Bonn, Brussels, Frankfurt, London, Luxembourg, Nicosia, Stockholm, Tunis, etc. The company designs, develops, supports and promotes software ICT applications using integrated, state-of-art technology to governments, public organizations and private enterprises in more than 27 countries in the world. Customers include government institutions, multinational corporations, public administrations and multinational companies, research and academic institutes. ED has an extended expertise in the areas of e-Government (they include Taxation, Customs, Statistics, Intellectual Property, Trade Marks, Patents, Pharmaceuticals, Health, Justice, etc.), e-Business, e- Procurement, e-Collaboration, groupware and workflow, content, document and knowledge management, communications middleware, ICT security. Own software products and tools have been developed in these domains. All the products and services are offered for web, intranet and Internet environments and are based on open architectures and state-of-the-art technologies.</p> <p>ED is an ISO 9001:2008 and ISO 27001:2005 certified company and holds a NATO and EU security clearance (secret).</p> <p>ED has expertise in the provision of SaaS, e-business (B2C, B2B, B2E, B2G, G2G, etc.), BroadBand Services, e-collaboration and workflow management, developing its own software applications and products, offered for web, Internet and portable devices, relying on open architectures. Its activities include the:</p> <ul style="list-style-type: none"> • successful delivery of a large number of IT complex projects to international organisations, such as the European Parliament, the European Court of Auditors, Interpol, the European Environment Agency (EEA) , the European Medicines Agency (EMA) , the Office for the Harmonisation of the Internal Market (OHIM), the European Police Office (EUROPOL) , the Publications Office of the European Union (POEU) , the European Centre for the Development of Vocational Training (CEDEFOP) , the European Chemicals Agency (ECHA) , the European Centre for Disease Prevention and Control (ECDC) and national administrations in Austria, Cyprus, Germany, Finland, Belgium, Bulgaria, The Netherlands, Italy, Switzerland, etc. • design and implementation of integrated ICT systems, e-Records warehousing, web interfaces, semantic and ontology support, “Object oriented” and n-tiers architectures including web services, SOA, ESB, etc., software total quality management, information systems security audit & design 				

Key Project personnel	
Publications Products, Services	<p><i>List of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p> <p><u>Commercial projects in the security domain</u> include:</p> <ul style="list-style-type: none">

	<ul style="list-style-type: none"> IT-based crises management exercises Federal Office of Civil Protection and Disaster <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>Commercial products of ED:</p> <ul style="list-style-type: none"> [REDACTED] <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Related projects	<p>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Equipment	<p>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</p> <p>N/A</p>
Any other documents	<p>Any other supporting documents, if specified in the work programme for this call</p> <p>N/A</p>

2. Institute of Communications and Computer Systems

NAME:	 Institute of Communication and Computer Systems (ICCS) – RF/Microwaves Wireless & Satcom Group				
Short Name:	ICCS	Country:	Greece	Partner #:	2
	Description				

General description of the org.	<p>The Institute of Communication and Computer Systems (ICCS) www.iccs.gr/eng/, established in 1989, is a non-profit Academic Research Body associated with the School of Electrical & Computer Engineering (SECE) of the National Technical University of Athens (NTUA) under the auspice of the Hellenic Ministry of Education. ICCS carries research and development activities in the fields of all diverse aspects of telecommunications, computer systems and techniques and their application in a variety of areas. ICCS personnel consists of a number of Senior Researchers and associated scientists, substantially supported by SECE University Professors. ICCS involves many Research Groups and Laboratories very active in National and European funded research projects.</p> <p>In iCROSS proposal, ICCS participates through the RF/Microwaves Wireless & Satcom Group, an active Research Group of the Microwave and Fiber Optics Laboratory (MFOL) of ICCS/NTUA. MFOL (http://mfol.ece.ntua.gr/), established in 1985 as one of the NTUA Laboratories and a research unit of ICCS, holds a long-standing track record on basic and applied research, design & development, testing and measurements of RF/microwave units and systems covering almost the entire electromagnetic spectrum. The RF/Microwaves Wireless & Satcom Group of MFOL owns extensive experience in the related fields and is involved in many National and EU projects. The Group's staff consists of 1 ICCS Senior Researcher, 3 Professors, 2 postdoc senior researchers and PhD students.</p> <p>The most important areas of R&D activities performed or supported by the Group involve design and development of: RF & microwave systems, remote sensing, radar, life detectors and sensors, satellite communication and wireless radio networks, antennas front-end and wireless systems and subsystems up to millimeter waves, signal processing, as well as applications relevant to telecom, satcom and broadband wireless networks with the development of many dedicated prototypes. The Group has significant expertise and know-how in wireless and satellite communication systems design, digital communications, radio network dimensioning and planning, radio coverage measurements, radio channel modelling, RF systems design, interference studies and measurements, spectrum management and radio protocols design. Finally, the Group owns a broad experience in Lab and on Site / Field measurements along with conductance of EMC/EMI tests (conducted/radiated emission / immunity tests, STANAG standards etc).</p> <p>The Group's staff are active members of the research community having published more than 500 publications in International Journals and Conferences in the above subjects. Members of the Group have been involved in more than 60 R&D projects funded either from EC or the Greek Public/Private Sector such as: E-SPONDER (FP7 SECURITY), Jason, WiSepon, Emosic and Maribrain (Cooperation I & II), NexGenMiliwave, EU-FP7 HIRF, FP7 interactIVe, FP6-RURAL WINGS, SATNEX I (FP6 IST), SATNEX II (FP6 IST), SATNEX III (ESA), MIMO-NPI, (ESA-NPI), Flame, MIMOSA and COST Actions.</p> <div data-bbox="350 1339 1344 1759" style="background-color: black; height: 200px; width: 100%;"></div>
Key Project personnel	<div data-bbox="350 1759 1344 1957" style="background-color: black; height: 100px; width: 100%;"></div>

RF/microwaves (1999, NTUA). She also holds Master in Business Administration (MBA,

[REDACTED]

[REDACTED]


[REDACTED]

[REDACTED]

[REDACTED]


[REDACTED]

Publications Products, Services	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p> <ul style="list-style-type: none"> • M. Bimpas, N. Paraskevopoulos, K. Nikellis, D. Economou and N. Uzunoglu "Development of a Three Band Radar System for detecting Trapped alive humans under building ruins", Journal PIER Vol 49, pp 161–188, 2004 • P. D. Arapoglou, K. P. Liolis, A. D. Panagopoulos, "Railway Satellite Channel at Ku Band and Above: Composite Dynamic Modeling for the Design of Fade Mitigation Techniques", Intern. Journal of Satellite Communications and Networking, Jan. 2012. • V. K. Sakarellos, C. Kourogiorgas, A. D. Panagopoulos, "Cooperative Hybrid Land Mobile Satellite–Terrestrial Broadcasting Systems: Outage Probability Evaluation and Accurate Simulation", Wireless Personal Comms, 79-2, pp 1471-1481, July 2014. • S. Enserink, A. D. Panagopoulos, M. Fitz, "On the Calculation of Constrained Capacity and Outage Probability of Broadband Satellite Communication Links", IEEE Wireless Communication Letters, pp. 453-456, Oct. 2014. • Cidronali...Makri, et al, "TX system-level analysis by behavioral modeling of RF building blocks: the IEEE802.11a/IEEE802.15.3a case studies" GAAS'05, EuMW • R. Makri, et al, "Next Generation mm-Wave Backhaul Radio: Overall System Design for GbE 60GHz PtP Wireless Radio of high CMOS Integration", IEEE ICECS'11 Conference, 2011 <p>Patents</p>

	<ul style="list-style-type: none"> GR20050100254, IPC G01S1/00, N.K. Uzunoglu, E. Alivizatos et al, «<i>Multistatic UHF Radar System for the detection of targets with very low radar cross section (RCS)</i>», May 2005 GR2003100417, IPC G03B15/00, N.K. Uzunoglu, K. Kassios et al, «<i>Evaluation arrangement for Landscape quality classification with artificial neuron networks</i>», October 2003, ICCS
Related projects	<p><i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i></p> <ul style="list-style-type: none"> 

Equipment	<p><i>Description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i></p> <p>The RF/Microwaves Wireless & Satcom Group, being a research group of the Microwaves and Fiber Optics Laboratory of ICCS/NTUA, has direct access to the MFOL's extensive Lab equipment involving portable Vector Network Analysers, Spectrum & Communication Analysers up to 50GHz along with mm-wave Sources and external mixers for 50 - 110 GHz including various frequencies antennas. Furthermore, for iCROSS purposes the Group will utilise the anechoic chamber for antenna measurements and EMC / EMI tests and the shielded enclosure / Faraday room facilities of MFOL. Other hardware equipment to be used for iCROSS involve:</p> <ul style="list-style-type: none"> - 2 Satellite Software Defined Receivers at Ka band - DVB-RCS terminal at Ka band - Transceivers at 60GHz transmission - IEEE 802.16m Base Station - 6 ETTUS USRPs - 3 Libelium Wi-Fi Scanners - Other software tools available such as Matlab, Simulink, LabView, Altium.
Any other documents	<p><i>Any other supporting documents, if specified in the work programme for this call</i></p> <p>N/A</p>

3. Stremble Ventures Ltd.

NAME:	 STREMBLE Ventures LTD			
Short Name:	STR	Country:	Cyprus	Partner #: 3
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>Stremble Ventures LTD is a Research and Development oriented company. Its goal is to bring together scientists from different disciplines and provide them with the resources needed to research and develop state-of-the-art technologies that transcend their expertise with the ultimate goal of transforming state-of-the-art research into beneficial products for European citizens. For the ENRICH project both the Advanced Analytics Department as well as the Educational Technologies department will be involved.</p> <p>The Educational Technology Department focuses on research and development with respect to ways in which Information and Communication Technologies (ICT) and new media (avatars, Web2.0 technologies, simulated environments) influence interaction and communication between users in formal and informal educational and other settings.</p> <div style="background-color: black; height: 150px; width: 100%;"></div>			

Key Project personnel				


--	--	--	--	--

A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content

Antoniades, A., Nicolaidou, I. Constantinou, R., Marangos, Ch., Kyriacou, E., Bamidis, P., Dafli, E. & Pattichis, C. (in press, 2015). The potential of a virtual

Publications Products, Services	<p>emergency telemedicine serious game in medical training: a quantitative, professional feedback informed evaluation study. <i>Journal of Medical Internet Research</i> (In Press 2015, impact factor: 4.7)</p> <p>Antoniades A., Georgousopoulos C., Forgo, N., ... Pattichis C.S., "<i>Linked2Safety: A secure linked data medical information space for semantically-interconnecting EHRs advancing patients' safety in medical research</i>," in IEEE 12th International Conference on Bioinformatics and Bioengineering (BIBE), Larnaka, Cyprus, 2012, DOI:10.1109/BIBE.2012.6399767, pp. 517-522, 2012.</p> <p>Nicolaidou, I., Antoniades, A., Myllari, J. Giordano, D., Dafli, E., Schizas, Ch., Nikolaidou, M., Spachos, D., Bamidis, P. & Pattichis, C. (2011). Evaluation methodologies in e-systems: A proposed evaluation framework and its application in medical education. In P. Bamidis, V. Anastasov & L. Despotova-Toleva (Eds). e-education & e-science, p. 87-112. Medical Publishing VAP. ISBN: 978-960-243-682-682-</p> <p>A.Lanitis, C.J. Taylor and T.F. Cootes. Automatic Interpretation and Coding of Face Images, UsingFlexible Models. IEEE Transactions of Pattern Analysis and Machine Intelligence, Special Issue in Face and Gesture Recognition Vol 19, no 7, pp 743-756, 1997.</p>
Related projects	<p><i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i></p> <p>[REDACTED]</p>
Equipment	<p><i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i></p> <p>N/A</p>
Any other documents	<p><i>Any other supporting documents, if specified in the work programme for this call</i></p> <p>N/A</p>

4. Manchester Metropolitan University

NAME:	 <p>Manchester Metropolitan University</p> <p>Manchester Metropolitan University</p>				
Short Name:	MMU	Country:	UK	Partner #:	4

<p>General description of the org.</p>	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>The Manchester Metropolitan University (MMU) is one the largest Universities in the UK, hosting 34,000 students and employing 4,300 staff. It is amongst the best performing ‘new universities’ for research. MMU has experience of participating in, and managing a range of European funded research projects including a number supported by previous Framework Programmes. The School in which the team are based (Computing, Mathematics and Digital Technology) currently co-ordinates the Framework 7 projects BACTOCOM, COBRA and TRUCE.</p> <p>MMU’s contribution will be led by the Intelligent Systems Group (ISG). ISG has expertise in using computational intelligence techniques (specifically artificial neural networks) to monitor and analyze visual non-verbal behaviour in human subjects. MMU holds a patent on technology in this area relating to the system Silent Talker (Publication number WO2002087443 A1, Application number PCT/GB2002/001806), which learns patterns of microgestures which can be used to detect deception. The group also has extensive experience in the development of Conversational Agents and Conversational Intelligent Tutoring Systems. It has conducted pioneering work in the development of short text semantic similarity measures (STSS) that has led to the development of semantic conversational agents and in addition the Multi-lingual STSS in Arabic, Urdu and Thai. Recent work in this area also includes the design of highly computationally efficient algorithms for classifying Dialogue Acts based solely on small vocabulary (function word) features. Members of the group also have extensive knowledge of computational intelligence techniques including computing with words, fuzzy logic and evolutionary algorithms and natural language Interfaces for database information retrieval systems.</p> <p>The project team will also have access to specialised facilities and equipment including a usability lab within MMU which incorporates a range of tools and techniques (eye tracking, sensing equipment, video recording and Noldus Observer XT10 behaviour analysis software) to analyse human behaviour.</p> <div data-bbox="350 1041 1343 1371" style="background-color: black; height: 150px; width: 100%;"></div>
<p>Key Project personnel</p>	<p><i>A CV or description of the profile of the persons, including their gender, who will be primarily responsible for carrying out the proposed research and/or innovation activities</i></p> <div data-bbox="350 1444 1343 1965" style="background-color: black; height: 250px; width: 100%;"></div>

novel goal-driven CA architecture used in a range of applications within a Higher

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]


Publications Products, Services	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p> <p>Rothwell, J. Bandar, Z. O'Shea, J. McLean, D. Silent talker: a new computer-based system for the analysis of facial cues to deceive Journal of Applied Cognitive Psychology, Volume 20, Issue 6, pages 757– September 2006. doi: 10.1002/acp.1204 This is the pre-peer reviewed version of the article which has been published in final form http://onlinelibrary.wiley.com/doi/10.1002/acp.1204/abstract</p> <p>Rothwell, J. Bandar, Z. O'Shea, J. McLean, D. Charting the behavioural state of a person using a Backpropagation Neural Network Journal of Neural Computing and Applications. DOI 10.1007/s00521-006-0055-9. 2 This is the pre-peer reviewed version of the article which has been published in form http://dl.acm.org/citation.cfm?id=1267004&CFID=80812022&CFTOKEN=673420</p> <p>Buckingham, F. Crockett, K. Bandar, Z. O'Shea, J. MacQueen, K. and Chen Measuring Human Comprehension from Nonverbal Behaviour using Artificial Neural Networks, Proceedings, WCCI 2012 IEEE World Congress on Computational Intelligence Australia, pp368-375, 2012 ISBN 978-1-4673-1489-3, 10.1109/IJCNN.2012.6252414</p> <p>Buckingham, F. Crockett, K. Bandar, Z. O'Shea, J., FATHOM – A Comprehension Monitoring System using Artificial Neural Networks, FATHOM: A neural network based non-verbal human comprehension detection system for learning environments IEEE SSCI, pp. 403 – 409, DOI: 10.1109/CIDM.2014.7008696, 2014. Rothwell J., Bandar Z., O'Shea J., McLean D. Analysis of the Behaviour of a subject UK Intellectual Property Office, WO 02/087443 A1. 2002.</p>
Related projects	<p><i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i></p> <p>[REDACTED]</p> <p>[REDACTED]</p>

[REDACTED]

A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work

Any other supporting documents, if specified in the work programme for this call
N/A

5. iTTi Sp. z o.o.

NAME:	 iTTi Sp. z o.o.
-------	---

Short Name:	ITTI	Country:	Poland	Partner #:	5
--------------------	------	-----------------	--------	-------------------	---

<p>General description of the org.</p>	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>ITTI sp. z o.o. is an SME working in IT and telecommunications sectors, located in Poznan, Poland. The company has at present a team consisting of 80 persons. The activities of ITTI can be grouped into three categories:</p> <ul style="list-style-type: none"> ▪ technical consulting in the area of telecommunications and IT - ITTI assists end-users (i.e. public administration, utilities, banks, companies) in purchasing, implementation and optimisation of IT and telecom systems; a number of professional methodologies are used in this area, e.g. PRINCE2, CISA, PMI, TOGAF, ITIL, ISO 27001, BS25999, UML; ITTI offers also its services to practically all key telecommunications players in Poland; ▪ applied R&D in the area of IT and telecommunications – ITTI contributes to the R&D projects providing the expertise in the following areas: user requirements, system design, data processing (ontologies, data mining), lessons learnt systems, graphical user interfaces, mobile applications, quality of service and quality of experience, cybersecurity, simulation of telecommunication networks, simulation of procedures in crisis situations; ▪ development of innovative applications and software solutions - ITTI designs and develops innovative solutions which are adjusted to customer needs (e.g. in crisis management and health sector). <p>ITTI carried out research activities in the following programmes: EU-funded initiatives, currently in the Horizon 2020 (formerly also FP7, FP6 and FP5), European Defence Agency programmes (e.g. Joint Investment Programme on Force Protection, Joint</p>
---	--


Investment Programme on CBRN) as well as Action Grant CIPS II and NATO Industrial Advisory Group studies. The company has also been active in some Polish applied research projects. Recently, ITTI has been also involved in the European Space Agency projects. In R&D activities the company cooperates closely with numerous universities and research institutes based in Poland as well as around Europe. Moreover, ITTI is **an institutional member** of the Public Safety Communication Europe Forum, Integrated Mission Group for Security (IMG-S) and ITIC Group - International Telecommunications and IT Consultants. ITTI is also one of the co-founders of Polish Space Industry Association and participates to Wielkopolska ICT Cluster. In the recent years ITTI was awarded the prestigious “Cristal Brussels Prize 2013” **for the most active and successful Polish company participating in FP7**, while in 2009 ITTI received the reward for high performance in R&D projects for the European Defence Agency awarded by the Polish Ministry of Defence.

[REDACTED]

[illegible][illegible]

	<div style="background-color: black; width: 100%; height: 40px;"></div> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="background-color: black; width: 15%; height: 20px;"></div> <div style="background-color: black; width: 40%; height: 20px;"></div> <div style="background-color: black; width: 15%; height: 20px;"></div> <div style="background-color: black; width: 30%; height: 20px;"></div> </div> <div style="background-color: black; width: 100%; height: 100px;"></div>			
Publications Products, Services	<i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i> N/A			
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i> <ul style="list-style-type: none"> ■ <div style="background-color: black; width: 60%; height: 20px;"></div> ■ <div style="background-color: black; width: 60%; height: 20px;"></div> ■ <div style="background-color: black; width: 60%; height: 20px;"></div> ■ <div style="background-color: black; width: 60%; height: 20px;"></div> ■ <div style="background-color: black; width: 60%; height: 20px;"></div> 			
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i> ITTII possesses the standard IT environment (i.e. workstations, servers, software tools). ITTI owns standard office equipment (laptops, computers, phones) and conference facilities (inter alia GoToMeeting licence). ITTI has also servers that can be used for testbeds. In ITTI there is also a team of software developers and programmers. ITTI has also long experience in development of software solutions in R&D projects at national and international level.			
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A			

6. Everis Aerospace and Defence


NAME:	<div style="display: flex; align-items: center;">  <div> Everis Aerospace and Defence </div> </div>				
Short Name:	EVR	Country:	Spain	Partner #:	6
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> EVERIS AEROESPACIAL Y DEFENSA is a multinational group born in Spain with a commercial network around the world that provides global solutions for				

Key Project personnel

	<div style="background-color: black; width: 100%; height: 150px;"></div> <div style="background-color: black; width: 100%; height: 100px;"></div>
<p>Publication s Products, Services</p>	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p> <p><u>Products and services:</u></p> <div style="background-color: black; width: 100%; height: 450px;"></div>

	<div style="background-color: black; width: 100%; height: 100%;"></div>
Related projects	<p><i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i></p> <div style="background-color: black; width: 100%; height: 100%;"></div>
Equipment	<p><i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i></p> <p>N/A</p>
Any other documents	<p><i>Any other supporting documents, if specified in the work programme for this call</i></p> <p>N/A</p>

7. BioSec Group Ltd.

NAME:	 <p>BioSec Group Ltd.</p>			
Short Name:	BIO	Country:	Hungary	Partner #: 7
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>BioSec Group Ltd. has been established by four private people with the only goal to develop biometric identification solution based on palm vein recognition. Positioned as R&D company, BioSec has created own software and hardware development infrastructure. Using indirect sales strategy, BioSec is represented in 13 countries all over the world and is specialized within biometric recognition in mass identification and IT security. Based on R&D experience since 2008, BioSec became one of the leading development companies for developing palm vein recognition based solutions. Number of employees is in total 19.</p> <p>Specialist areas of expertise of BioSec can be summarised as follows:</p> <ul style="list-style-type: none"> ▪ software development in C#, specialized in biometric recognition ▪ data encryption ▪ creating physical security systems ▪ hardware development for mobile devices ▪ mass handling ▪ planning and implementing large scale security systems ▪ system integration <div data-bbox="349 989 1343 1255" style="background-color: black; height: 127px; width: 100%;"></div>			
Key Project personnel	<div data-bbox="349 1255 1343 1556" style="background-color: black; height: 143px; width: 100%;"></div> <div data-bbox="349 1598 1343 1885" style="background-color: black; height: 137px; width: 100%;"></div>			

	<div style="background-color: black; width: 100%; height: 100%;"></div>
Publication s Products, Services	<i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i>
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i> <div style="background-color: black; width: 100%; height: 100%;"></div>
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i> <p>As R&D company, BioSec has its own highly developed and equipped laboratory for testing software and hardware elements.</p> <p>Technical equipment includes:</p> <ul style="list-style-type: none"> • software laboratory <ul style="list-style-type: none"> ○ simultaneous software testing ○ stress testing ○ vulnerability tests • hardware laboratory <ul style="list-style-type: none"> ○ simulation of outdoor conditions ○ stress testing
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A

8. JAS technologie sp z o.o. (Ltd)

NAME:	 JAS technologie sp z o.o. (Ltd)				
Short Name:	JAS	Country:	Poland	Partner #:	8
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> <p>JAS technologie Sp. z o.o. (Ltd) is dynamically growing technology company, operating in telecommunication and security. The company is owned in 100% by Polish capital. The company works closely with equipment manufacturers, Polish Government, Polish Air Navigation Services Agency, Research & Development organizations and Defense</p>				

	<p>Contractors to address their requirements regarding technical expertise, consultancy and business process support.. In subject areas where JAS technologie is active, we continually monitor the local market space and the markets abroad. JAS technologie takes an active part in tradeshows, exhibitions and conferences on defense and security industry including i.a. EUROPOLTECH (International Fair of Technology and Equipment for the Police and National Security Services), The International Defence Industry Exhibition (with Honorary Patronage of the President of the Republic of Poland) and International Conference and Exhibition. JAS cooperate with major research centres in Poland, such as Military University of Technology (WAT), Warsaw University of Technology (PW), The Main School of Fire Service (SGSP), Military Institute of Chemistry and Radiometry (WICHiR), Scientific Research Centre of Fire Protection - State Research Institute (CNBOP-PIB), The National Institute of Telecommunication - State Research Institute (IL-PIB). Among the entities JAS cooperates in particular with the Ministry of Internal Affairs (MSW) and entities subject: Police, Fire Department, Border Guards and The Government Protection Bureau (BOR).</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>								
<p>Key Project personnel</p>	<table border="1"> <tr> <td data-bbox="350 1184 748 1299">[REDACTED]</td><td data-bbox="748 1184 1343 1299">[REDACTED]</td></tr> <tr> <td colspan="2" data-bbox="350 1299 1343 1814">[REDACTED]</td></tr> <tr> <td data-bbox="350 1814 748 1856">[REDACTED]</td><td data-bbox="748 1814 1343 1856">[REDACTED]</td></tr> <tr> <td colspan="2" data-bbox="350 1856 1343 1953">[REDACTED]</td></tr> </table>	[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]								
[REDACTED]									
[REDACTED]	[REDACTED]								
[REDACTED]									

Publications Products, Services	<i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i>			
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i>			
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i>			
	As part of its work in R & D projects the company has made purchases of biometric hardware and dedicated software for the tasks. JAS also has adequate facilities to support the IT hardware programming work. In the implementation of tasks in R & D projects as well as commercial projects, JAS cooperates with many equipment suppliers in Poland and abroad.			
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i>			
	N/A			


9. Gottfried Wilhelm Leibniz Universitaet Hannover

NAME:	 Leibniz Universität Hannover			
Short Name:	LUH	Country:	Germany	Partner #: 9
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> The Institute for Legal Informatics (IRI), being part of LUH's School of Law, was established in 1983 and is the first Institute dedicated to scientific research on all issues of Information and Communication Technologies at a German University.			

	<p>With currently more than 40 people staff IRI is one of Europe's largest institutions in the field and is actively involved in about 10 European research projects with a focus on data protection, data security and intellectual property. Nikolaus Forgó has been leading IRI in cooperation with Prof. Dr. Heinze since 2014. The L3S Research Centre, also part of LUH, focuses on fundamental and application-oriented research in all areas of Web Science and has a focus on computer science. L3S researchers develop new methods and technologies that enable intelligent, seamless access to information via the Web; link individuals and communities in all areas of the knowledge society, including academia and education; and connect the Internet to the real world. Since 2008, the L3S has been involved in 12 EU projects as part of the EU's Seventh Framework Programme, four of them (LivingKnowledge, Okkam, EUWB and EERQI) integrated projects, as well as the STELLAR Network of Excellence.</p> <div data-bbox="347 600 1344 961" style="background-color: black; height: 170px; width: 100%;"></div>
<p>Key Project personnel</p>	<div data-bbox="347 968 1344 1808" style="background-color: black; height: 400px; width: 100%;"></div>
<p>Publications Products, Services</p>	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p>


	<p>1. Betrieblicher Datenschutz Rechtshandbuch [Handbook operational Data Protection] (Nikolaus Forgo, Marcus Helfrich, and Jochen Schneider (editors)), Munchen: Beck 2014, 1035 pages</p> <p>2. Dealing with Data Safety and Security in Translational and Personalized Medicine (together with Norbert Graf, Yvonne Braun, Elias Neri, Brecht Claerhout et al), in: Pediatric Blood & Cancer 2013, vol. 60, no. 3; doi: 10.1002/psc.24719</p> <p>3. Security Issues in research projects with patient's medical data (together with M. Goralczyk, and Constantin Graf von Rex), in: Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), Larnaca, Cyprus, 11-13 November 2012, pp. 541-546</p> <p>4. Legal issues in clouds: towards a risk inventory (together with K. Djemame, B. Barnitzke, M. Corrales, M. Kiran, M. Jiang, D. Armstrong and I. Nwankwo), in: Philosophical Transactions of the Royal Society A, A 2013 371, 20120075</p> <p>5. Assuring Data Privacy in Cloud Transformations (together with Corrales, Nwankwo and others), in: Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on Digital Object Identifier, pp. 1063 – 1069</p>
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i>
Equipment	<p><i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i></p> <p>N/A</p>
Any other documents	<p><i>Any other supporting documents, if specified in the work programme for this call</i></p> <p>N/A</p>

10. Országos Rendőr-főkapitányság (Hungarian National Police)


NAME:	 <p>Országos Rendőr-főkapitányság</p>				
Short Name:	HNP	Country:	Hungary	Partner #:	10
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>The Hungarian National Police is the only police agency in Hungary, with more than 42,000 sworn members. It undertakes all policing duties within Hungary, including criminal investigation, patrol activities, traffic policing and border control. It is led by the National Police Commissioner under the control of the Minister of the Interior. The body is divided into county police departments, with a further subdivision into regional and town police departments. County police departments and some special units are affiliated legal entities. It is also the agency which operates the 112 national emergency response system, called the ESR. (The Hungarian Border Guard was integrated into the HNP in 2008.)</p> <p>Border control duties are coordinated by the General Department of Border Control and carried out by 67 Border Police Outposts and 85 BCPs along the external border as well as inland alien policing units, consisting of 3500 uniformed professionals in total.</p>				

	<p>Specialist areas of expertise of the HNP can be summarised as follows:</p> <ul style="list-style-type: none">▪ Law-enforcement, including public policing, criminal investigation, traffic policing and border control.▪ Operating the situational network (112) centre covering all of Hungary.▪ Own risk analysis department.▪ More than 120 years of experience in policing.▪ Experience in policy making and supervision in the area of aviation security.▪ Strong international cooperation capabilities (liaison officers, attachés, National Contact Point etc.).▪ Sound experience in training staff in the use of the e-learning network.▪ Use of different media to inform public (press officer network), good connection to key players. <p>[REDACTED]</p>						
	<p>[REDACTED]</p> <table><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr></table> <p>[REDACTED]</p> <table><tr><td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr></table> <p>[REDACTED]</p>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]					
[REDACTED]	[REDACTED]	[REDACTED]					
<p>Publications Products, Services</p>	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p> <ul style="list-style-type: none">▪ SZÉKELY Zoltán (2014), Schengen: At the Border and Beyond: Past, present and future In: NISPACee (ed.), <i>Government vs. Governance in Central and Eastern Europe: From PreWeberianism to NeoWeberianism?</i>, 22st NISPACee Annual Conference; XII. Working Group on Administration & Management of Internal						

	<p>Security Agencies. Conference held at: Budapest, Hungary, 2014.05.22-2014.05.24. Bratislava: NISPACE, 2014. ISBN:9788089013722</p> <ul style="list-style-type: none"> ▪ NAGY Judit, SZEKELY Zoltán (2014), Police Robots and the Prüm Convention: Compliance Study on Police Robots and Freedom of Information, In: Péter Korondi (ed.) Proceedings of ARES14: Workshop on Application of Robotics for Enhanced Security. Conference held at: Budapest, Hungary, 2014.06.13-2014.06.14. Budapest: Budapest University of Technology and Economics, 2014, pp. 16-20. ISBN:9789633131282 ▪ SZÉKELY Zoltán: Habeas Corpus Machinima – Elfoghat-e engem egy robot? [May a robot arrest me?] In: <i>Hadmérnök [Military Engineer]</i>, Vol. IX. (2014) No. 1., pp. 291-303, ISSN 1788-1919 ▪ SZEKELY Zoltán (2013), Repülők és határok régen és ma [Airplanes and borders in the past and in present] <i>Rendvédelem-történeti Füzetek [Law Enforcement History Journal]</i> XXIII. : (30.) pp. 179-186. ISSN 1216-6774 ▪ NÉMETH József: The role of the Bureau of Border Patrol and its tasks against the terrorism: Domestic and international opportunities. <i>ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE</i> 6: pp. 623-629. p. 6 (2007)
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i>
Equipment	<p><i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i></p> <p>The HNP is responsible for about 14% of total Schengen Area land borders (~1100 km out of ~7700 km), dealing with 7% of total cross-border traffic of the EU (~32 million per year out of ~480 million per year). This task is carried out with 3500 uniformed border police professionals with state-of-the-art technical equipment at enlarged or newly constructed Outposts and Border Crossing points.</p> <div style="background-color: black; width: 100%; height: 100%; min-height: 300px;"></div>








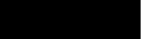


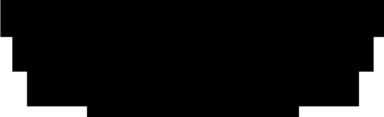






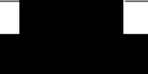
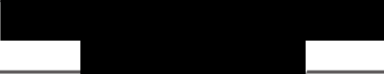


	
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A

11. Polish Border Guards


NAME:	 Karpacki Border Guard Support Center of Polish Border Guard - Headquarters of Polish Border Guard			
Short Name:	PBG	Country:	Poland	Partner #: 11
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>Border Guard, in accordance with Art. 1 of the Act of 12 October 1990 on the Border Guard, is a unitary, uniformed and armed formation.</p> <p>Polish Border Guard within its duty carries out tasks aimed at:</p> <ul style="list-style-type: none"> • Organising the border checks to ensure fluidity movement of people and means of transport across the state border taking place in accordance with the law, while maintaining high efficiency detection of crimes and offenses in this area, • protection of the state border on land and sea, • organizing and carrying out border traffic control, • Recognition, prevention and detection of offenses and prosecution of their perpetrators, within the jurisdiction of the Border Guard, in particular: <ol style="list-style-type: none"> 1. offenses related to crossing the state border in compliance with the provisions related to the reliability of documents entitling to cross the state border, 2. crimes against public safety and security, offenses in communication in connection with the performance of air transport 3. cooperation with other authorities and services in the field of recognizing the risk of terrorism and countering any of these threats, 4. the gathering and processing of information for the protection of the state border-entry, and exchanging of those information with the competent authorities of the state, 			

	<ol style="list-style-type: none"> 5. Border Guard carries out tasks under the law of the European-Union and international agreements on principles and scope set out in them, 6. cooperation with other Member States and the Community joint ventures within the working groups 7. Striving to undertake many actions financing from EU funds and bridging funds. <p>According to Order No. 1 of the Border Guard Commander in Chief of 14 January 2014 on the establishment of the Karpacki Border Guard Support Center (KBGSC) in Nowy Sacz, our unit performs tasks throughout the country on behalf of other units of the Polish Border Guard. KBGSC is an entity having the potential of human resources and organizational - logistics to carry out the Project BES-6-2015 under the Horizon 2020 Programme. Supporting character of the KBGSC in Nowy Sacz allows to carry out a nationwide recruiting of the officers from different units of the Border Guard performing tasks on different state borders sectors (land, air and sea), and subsequently, will coordinate all implemented tasks of the Project.</p> <p>Due to the fact that Poland is an external border of the European Union and the length of the land border is 1163.25 km (state border between Poland and Russian Federation, Republic of Belarus, Ukraine) with the one main airport and ten regional, the necessity to improve tools and methods for border control with the implementation of biometric technologies, i.a. in the context of automated border control systems is the main objective of the development strategy for Polish Border Guard.</p> <p>PBG closely associated with the implementation of research projects under the National Center for Research and Development.</p> <p>PBG set up within its structure a scientific-technical council that compile thematic issues that are referred to consider innovation.</p> <p>Works within the National Center for Research and Development enable active participation of PBG in the development process as an adviser/expert.</p> <div data-bbox="349 1100 1344 1360" style="background-color: black; height: 124px; width: 613px;"></div>
<p>Key Project personnel</p>	<div data-bbox="349 1415 1344 1959" style="background-color: black; height: 259px; width: 613px;"></div>

	<div data-bbox="349 107 1344 527" style="background-color: black; width: 100%; height: 100%;"></div>
<p>Publication s Products, Services</p>	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p> <div data-bbox="381 590 1344 1965" style="background-color: black; width: 100%; height: 100%;"></div>

					
Related projects	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i>				
	no.	Name of the Fund	Name of the Project	Value of the Project	Implementation period
	1				
	2				
	3				
	4				
	5				
Equipment	<p><i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i></p> <p>The PBG has a comprehensive infrastructure and facilities of technical equipment enabling the conduct efficient and coordinated border control both in land air and sea movement.</p> <p>The whole was integrated in the four-level management system of the external border of the European Union / Schengen.</p>				
Any other documents	<p><i>Any other supporting documents, if specified in the work programme for this call</i></p> <p>N/A</p>				

12. TRAINOSE METAFORES – METAFORIKES YPIRESIES EPIVATON KAI FORTIOU AE

NAME:	 TRAINOSE METAFORES – METAFORIKES YPIRESIES EPIVATON KAI FORTIOU AE				
Short Name:	TRA	Country:	Greece	Partner #:	12
General description of the org.	<p><i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i></p> <p>TRAINOSE S.A. was established on 2005 initially as a subsidiary of OSE S.A. group. Since 2007 TRAINOSE S.A. has undertaken the operation and exploitation of all the transportation activities (passenger, freight, etc) and it has been operating as an independent company, being separately managed and organized, according to the provisions of the EU legislation.</p> <p>The company is a member of the International Union of Railways (UIC), the Community of European Railway and Infrastructure Companies (CER), the International Rail Transport Committee (CIT) and the Forum Train Europe; whereas it vigorously continues its effort for international networking, in order to draw valuable and specialized technical know- how.</p> <p>The main scope of the company includes nowadays:</p> <ul style="list-style-type: none"> • The development, organization and exploitation of the urban, suburban, regional, intercity and international passenger and freight railway transportation, as well as all kinds of transportation using fixed track systems. • The development, organization and exploitation of multimodal transportation. • The development, organization and exploitation of urban, suburban, regional, intercity and international passenger and freight bus transportation, nationally and abroad. • The provision of all kinds of logistics services, as well as all related services. • The organization, exploitation and provision of bedding and catering services to passengers. • The provision of consulting services relating to activities in accordance with the scope of the company. <p>Its mission being sustainable development, TRAINOSE S.A. aims to provide its customers with:</p> <ul style="list-style-type: none"> • Reliable transportation • Clean and comfortable trains • On time and reliable information • Experienced and friendly staff <p>R&D activities are coordinated by the Strategic Planning Division of TRAINOSE, and since 2012 the company has been involved as a partner in several EU projects, mainly in the pilot tasks, which subsequently offers as a service to its clients. TRAINOSE emphasizes in the fields of research and technological development for the design, development and implementation of high added value services towards its clients.</p> <p>The active participation of TRAINOSE in EU projects enhances the skills of company staff through the exchange of expertise with other European rail operators, widens the network of associates and increases the company's competitiveness, while supporting the national strategies in the field of rail and combined, multimodal transportation.</p> <p>By now, TRAINOSE has finalized its participation to seven (7) European funded research projects being affiliated to previous EU initiatives, while has just started</p>				

its processes in one more project of Horizon 2020 EU Framework Programme, all of them summarized in the table below:

Project Name	European Initiative	Duration	Budget TRAINOSE SA. (EUR)
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]


Key Project personnel

[REDACTED]

	<div data-bbox="349 107 1338 409" style="background-color: black; height: 144px; width: 609px;"></div> <div data-bbox="349 409 1338 772" style="background-color: black; height: 173px; width: 609px;"></div> <div data-bbox="349 772 1338 1234" style="background-color: black; height: 220px; width: 609px;"></div> <div data-bbox="349 1234 1338 1709" style="background-color: black; height: 226px; width: 609px;"></div>
Publications Products, Services	<i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i>
	<i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i> <div data-bbox="349 1927 1338 1967" style="background-color: black; height: 19px; width: 609px;"></div>

Related projects	<div style="background-color: black; width: 100%; height: 150px;"></div> <div style="background-color: black; width: 100%; height: 100px;"></div> <div style="background-color: black; width: 100%; height: 150px;"></div> <div style="background-color: black; width: 100%; height: 50px;"></div>
Equipment	<i>A description of any significant infrastructure and/or any major items of technical equipment, relevant to the proposed work</i> N/A
Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A

13. State Border Guard of the Republic of Latvia

NAME:	 State Border Guard of the Republic of Latvia				
Short Name:	BSG	Country:	Latvia	Partner #:	13
General description of the org.	<i>Description of the legal entity and its main tasks, with an explanation of how its profile matches the tasks in the proposal</i> State Border Guard of the Republic of Latvia (BSG) is a direct administration State institution, under the supervision of the Ministry of the Interior. On issues of				

	<p>guarding and control of the State border, as well as on issues, which are associated with the control of the observance of the entry, residence, exit and transit of aliens and stateless persons regulations, and other issues within the competence.</p> <p>[REDACTED]</p>						
Key Project personnel	<p><i>A CV or description of the profile of the persons, including their gender, who will be primarily responsible for carrying out the proposed research and/or innovation activities</i></p> <table border="1"> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> </table> <p>[REDACTED]</p> <table border="1"> <tr> <td>[REDACTED]</td><td>[REDACTED]</td><td>[REDACTED]</td></tr> </table> <p>[REDACTED]</p>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]					
[REDACTED]	[REDACTED]	[REDACTED]					
Publications Products, Services	<p><i>A list of up to 5 relevant publications, and/or products, services (including widely-used datasets or software), or other achievements relevant to the call content</i></p>						
Related projects	<p><i>List up to 5 relevant previous projects or activities, connected to the subject of this proposal</i></p> <p>[REDACTED]</p> <p>[REDACTED]</p>						

Equipment

Any other documents	<i>Any other supporting documents, if specified in the work programme for this call</i> N/A

4.2. Third parties involved in the project (including use of third party resources)

Please complete, for each participant, the following table (or simply state “No third parties involved”, if applicable):

The following table concerns all participants of the iCROSS consortium.

Does the participant plan to subcontract certain tasks (please note that core tasks of the action should not be sub-contracted)	Y
Does the participant envisage that part of its work is performed by linked third parties ⁷⁵	N
Does the participant envisage the use of contributions in kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)	N

⁷⁵ A third party that is an affiliated entity or has a legal link to a participant implying a collaboration not limited to the action (Article 14 of the Model Grant Agreement).

Section 5: Ethics and Societal Impact

During the proposal preparation stage the relevant partners conducted a preliminary ethical requirements collection and platform review to identify any ethical or legal issues relevant to the planned development or deployment of iCROSS. This has resulted in a design for iCROSS that meets and surpasses legal and ethical requirements.

Specifically, the iCROSS consortium includes a partner institution expert in legal informatics, data protection, data security and ethics (LUH) who will lead the EU-wide legal review and legal and ethical compliance task. Any issues identified as part of this task will be addressed, either by incorporating them as requirements that need to be adhered to by the design and implementation of the iCROSS platform or by actions taken as part of this task such as the creation of legal documentation to be developed as part of this task and applied to any of the other tasks in the project. An example of this would be the need to provide informed consent to all Pilot or empirical data collection participants, to communicate with regulatory bodies such as data protection authorities and to report issues directly to the project coordinator and the general assembly.

Ethical privacy concerns are addressed through a privacy-by-design and privacy-by-default approach followed in the iCROSS data collection procedures to ensure that no legal or ethical issues arise in the course of the project execution. Risk management procedures are in place to address any now unforeseen issues. Informed consent materials will be developed as part of the project and will include both informative/educational material relevant stakeholders will go through to understand and be informed of their rights before they provided the consent.

The consortium agrees that proposals for Horizon 2020 need to demonstrate how innovative research can tackle the major societal challenges identified in the Europe 2020 strategy. Social Sciences and Humanities research can play an important and positive role in this process and indeed is uniquely placed to ensure that ethics is central in dealing with the normative dimensions of the themes and topics mentioned in Horizon 2020. Secure Societies targets the area of freedom, security and justice, without internal frontiers, as the European Agenda on Security (released on 28th of April, 2015) underlines

Europeans need to feel confident that, wherever they move within Europe, their freedom and their security are well protected, in full compliance with the Union's values, including the rule of law and fundamental rights. In recent years new and complex threats have emerged highlighting the need for further synergies and closer cooperation at all levels.

It has been noted that:

Horizon 2020 has ambitious aims that not only presuppose empirical claims, e.g., with respect to natural resources, available technologies or existing infrastructures, but also set specific goals, e.g., regarding sustainability, health and well-being, food production, the bio-based economy, and resource efficiency. These goals show that the research themes are not aims in themselves, but means to realising European commitments to human rights and values. These rights and values presuppose normative claims about how humans should treat one another, what makes for good society, and how responsible governments and businesses should behave.

The consortium is also dedicated to ensure full compliance with fundamental rights as required by the Lisbon Treaty – European Charter of Fundamental Rights – which came into force 1st December 2009), provide transparency, accountability as well as providing results compatible with the Prüm framework and the new Europol mandate. To achieve balance within “Liberty and Security” as a single fundamental right, we have decided to set up a sound ethical framework, which is not only essential in fostering responsible research and innovation but also key of providing results able to gain public legitimacy, becoming a widely accepted tool for border traffic control. This section elaborates on how this is operationalised in the iCROSS project.

1. Code of Ethics and Ethics Advisor

In order to ensure that all partners act along the same inline, a Code of Ethics is elaborated, containing rules on general ethics principles, data protection and transparency. It provide rules on the informed consent, procedures implemented for data collection, storage, protection, retention and destruction including confirmation that they comply with national and EU legislation. Legal entities as members of the consortium have to give written informed consent on the Code of Ethics as well as individual researchers participating in the project. The Code of Ethics also contains the Data Protection Rules which has to be applied through the entire implementation (see chapter on Data Protection). An independent Ethics Advisor, who is not employed at any of the consortium members, will be contracted to carry out training, counselling, monitoring and auditing activities in order to ensure that all phases of implementation are in line with the Code of Ethics. The Security Officer will support the work of the Ethics Advisor with taking the role of an internal Data Protection Officer with tasks and responsibilities detailed in the Data Protection Rules. Arbitration over ethics and data protection regulation will be carried out by an Ethics Committee chaired by a Chairman from one of the consortium partners with two members, the Ethics Advisor and the Data Protection Officer (Security Officer). The Committee resolves all cases in written decision and submits a report on ethics and data protection during the reporting period. In case of lack of consent, the Ethical Advisor has the right to write a parallel report.

2. Data Protection

As mentioned in the previous chapter, in general, data protection will be ensured within the frame of the Code of Ethics, in form of Data Protection Rules annexed to the Code. All partners and individuals participating in the research have to give informed consent on data protection rules as well as volunteers participating in the tests.

The procedure of giving informed consent consists of three steps and is coordinated by the Data Protection Officer, who:

- a. informs the persons about the project and the type of data required,
- b. distributes electronic copies of Data Protection Rules and answers all related questions, explains content of the rules as requested,
- c. collects and stores signed forms of informed consent in a searchable format.

It has to be highlighted, that the Hungarian National Police is empowered by law to collect, store and process personal data for the following purposes (Act XXXIV. of 1994 on The Police, 77.):

- a. border control and policing,
- b. crime prevention, fight against crime and terrorism.

For this reason, personal data of third country citizens crossing the border to or from Hungary are collected, stored and processed by the Hungarian National Police for 5 years from the day of border crossing (Act XXXIV. of 1994 on The Police, 91/L. §), affecting the following types of data:

- a. full name
- b. date of birth
- c. nationality
- d. gender
- e. passport number and type
- f. visa number and type

This is also affecting travellers who do not participate in iCROSS tests. If a volunteer revokes its volunteering for participation and informed consent on data processing in the frame of iCROSS, it has to be informed that in case of border crossing to or from Hungary, the personal data listed above will be still processed on the abovementioned legal basis.

All other types of personal data can only be processed on the basis of consent and all other participants can only process those within the frame of the Data Protection Rules. A register will be set up for each

participant by the Data Protection Officer recording data types processed and individuals having access to those data.

For example, capturing of video-audio conversation with an avatar has to be executed only after the user of the device capable of capturing this conversation (eg. laptop with webcam and microphone) has given permission to the relevant software to carry out the capturing sequence. Most operating systems have their built-in procedures to achieve user permission; our solution will use those built-in dynamic linkable libraries and other such tools to ask for the permission of the user. The same applies for other data collection in relevance of the use of the traveller's personal computing devices (eg. GPS data, actual mobile network, handshake with tokens etc.).

After the duration of data process period expires (5 years in total) or the informed consent has been revoked (the sooner applies), all personal and sensitive data has to be deleted from the databases of the consortium with proper software and/or hardware procedures rendering unauthorized restoration impossible (eg. DiskWipe, HDDerase, KillDisk, Format Command Write Zero Option etc.). In case any partner has a parallel, legal bases obligation to further process any kind of data, those partner will further process the data on the given legal basis, while all other partners shall carry out the deletion process. Before deletion, the Ethical Committee has to be notified in due time to be able to observe the procedure and the Security Advisory Board has to be informed on the relevant data to ensure it will be also removed from deliveries (reports). The detailed regulations on storage, process and deletion can be found in the Data Protection Rules (Art. 10.) part of the Ethics Code.

3. Incidental findings

In case the system or the border control personnel detects anything illegal when checking a person participating in the iCROSS as volunteer and crossing the border, two different types of actions may apply depending on the conditions:

- a. the persons shows a Letter of Commission (serialized and registered document with title "Nyílt Parancs" or "Megbízólevél") issued by the Hungarian National Police, the Hungarian National Protection Service or by the Hungarian Ministry of Interior that he or she has performed the action resembling on an illegal act of the sole purpose of testing the system, and the act committed is exactly as outlined in the commission document, in that case, no actions other than the normal border control has to be carried out with the illegal act ignored,
- b. otherwise, the person has to be handed over to the border police units present who will carry out standard operational procedures determined by regulations on the given case, and all relevant data has to be secured and handed over to the police as evidence, including those who were collected with the perpetrators consent (Act XIX. of 1998 on Penal Procedures 117.§ (2)).

In both cases, the Security Officer has to be informed, and he or she must register the transfer of personal data in the Data Transfer Registry.

Any other incidental findings, not happening at the border and/or in presence of police officers, for example video collected on known terrorist suspects, devices connecting from areas under insurgent control, videos collected on persons known (wanted) as kidnapped or lost, have to be handed over to the Hungarian National Police through the Security Officer.

4. Additional measures on profiling to avoid stigmatization

The main difference between profiling and stigmatization is that a stigma implies the presumption of bad intention or disgrace, while profiling is the act or process of learning information about someone based on what is already known, determining the way how we will check the person. Profiling does not only filters criminals, terrorist or illegal migrants, on the contrary, it has more effect on victims of human trafficking and regular travellers in scope of third country citizens. A recent handbook on human trafficking for example provides clear datasets on from which country which type and age of women are trafficked, how many of them are in one group, what are the main travel destinations. Regular travellers can pass through the border faster as the passport checking personnel already are knowing their profile, a few words on their

language and they already got their passport back, checked and stamped, without any further questioning about purpose of stay, means of stay etc. Sometimes the best profiling is to have clear profiles on regular travellers and filter out everything that is uncommon. However, profiling can also be exploited and misused, like any other tool. To provide additional measures on profiling to avoid stigmatization, we intend to add the following functions into the profiling system:

- a. lapse of scores – both positive and negative scores obtained according to the profiles will diminish with time, in accordance with the legal principle of limitation,
- b. diminishing returns – when travelling many times in very short time period, the basic positive score obtained by successful border crossing will decrease linearly, preventing exploitation of the good scores achievable with travelling regularly,
- c. random score element – a random one-time score with random prefix (positive or negative) will be added each time the profile is checked at the border, the possible values (random interval) will be set to contribute half the score needed for one step change in the control category (minimal, thorough, thorough in a separated place – according to the Regulation 562/2006/EC on the Schengen Border Code),
- d. no manual modification – nobody's score can be modified manually, values apply automatically when the conditional phenomena/case/decision is recorded.

5. False positives

This system does not make decisions on admission or refusal. Its sole purpose is to facilitate border crossing with giving information to both traveller and border guard. Therefore false positives do not have any legal effect, as the final decision is in the hand of the traveller (on travelling or not) and in the border guard (to determine level of control and decide about admission). This is mainly because the international, EU and national law has certain exceptions on persons which are so dynamic that is not programmable. For example once a diplomat from Angola flew to Budapest to participate on a ceremony before she proceeds to Russia to work on the embassy in Moscow, but the database showed she has an alert for refusal on her, because seven years before she was arrested for delivering illicit sexual services in a bar in Budapest. Although the alert was still valid for three more years, the Minister of Interior decided to lift the ban in respect of the change in the status of the person. In another case, a plane full of US soldiers from a non-NATO unit got engine problems and had to spend two days at Budapest Airport with repairs, but the soldiers did not have travel document with themselves. However, the border official in charge decided to let them enter the country and spend the night in a hotel instead aboard of the plane. Therefore iCROSS will tell the traveller, that what he or she can expect at the border, based on the information provided (eg. passport is expired, additional visa is required etc.), but will not tell him or her to travel or not to travel. The same applies for the border guard, iCROSS will only report information gathered, checks already made (eg. passport is valid, the person is identified), profile assessment results (in form of recommended level of control), but will not and is not allowed to tell the policeman what to do exactly, how to control the person and what shall be the decision.

ICROSS

*Code of Ethics
with annexed
Data Protection Regulations
and forms of informed consent*

closed on 02 March 2016

by



Annexes:

1. Data Protection Regulation
2. Declaration of individuals and of legal entities accepting Ethics Code and Data Protection Regulations (forms of informed consent)
3. Data process register and access table

Contents

PREAMBLE	104
SCOPE	104
EFFECT	104
RULES OF PARTICIPATION IN THE RESEARCH	104
DEFINITIONS AND PRINCIPLES	105
OBLIGATIONS FOR PARTICIPANTS	106
ETHICAL COMMITTEE	106
ANNEX 1 DECLARATION OF ACCEPTING THE ETHICS CODE	109
I. ANNEXES	112
ANNEX 1 DATA PROTECTION RULES FOR PROJECT 'ICROSS'	112
<i>Preamble</i>	<i>112</i>
<i>Article 1 Definitions.....</i>	<i>113</i>
<i>Article 2 Principles.....</i>	<i>114</i>
<i>Article 3 Criteria For Making Data Processing Legitimate.....</i>	<i>114</i>
<i>Article 4 Processing Sensitive Personal Data</i>	<i>115</i>
<i>Article 5 Information To Be Given To The Data Subject.....</i>	<i>115</i>
<i>Article 6 The Data Subject's Right Of Access To Data.....</i>	<i>116</i>
<i>Article 7 The Data Subject's Right To Object.....</i>	<i>117</i>
<i>Article 8 Confidentiality And Security Of Processing</i>	<i>118</i>
<i>Article 9 Transfer Of Personal Data To Third Countries.....</i>	<i>118</i>
<i>Article 10 Internal Data Protection Officer</i>	<i>119</i>
<i>Article 11 Other Provisions</i>	<i>120</i>
ANNEX DECLARATION OF ACCEPTING THE ETHICS CODE INCLUDING THE DATA PROTECTION RULE	122

Preamble

[REDACTED]

[REDACTED]

[REDACTED]

Scope

[REDACTED]

[REDACTED]

[REDACTED]

Effect

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Rules of participation in the research

[REDACTED]

[REDACTED]

[REDACTED]

Definitions and principles

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Obligations for participants

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Ethical Committee

[REDACTED]

[REDACTED]

100

© 2004 Blackwell Publishing Ltd

1. *Journal of Management Studies*, 1990, 27, 1, 1-14.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Annex 1

Declaration of accepting the Ethics Code

(for individuals and for legal entities, on separate pages)

<Page intentionally left blank>

DECLARATION

on accepting the Ethics Code for individuals

I, <NAME>, born in <POB> on
the <DOB> hereby declare that I have read and accept the Ethics
Code including the data protection rules of the project 'iCROSS' and I understand my rights and
obligations related to the project.

.....
<SIGNATURE>

.....
<DATE>

In witness whereof:

..... <NAME>
..... <ADDRESS>
..... <SIGNATURE>

..... <NAME>
..... <ADDRESS>
..... <SIGNATURE>

DECLARATION

on accepting the Ethics Code for legal entities

Name of Legal Entity:.....

Seat of Legal Entity:.....

Registration number:.....

VAT number:

PIC number:

represented by<NAME and POSITION>

hereby declares that the above mentioned legal entity accepts the Ethics Code including the data protection rules of the project 'ICROSS' of the project 'ICROSS' and understands the rights and obligations related to the project.

.....

<DATE>

.....

<SIGNATURE and STAMP>

I. Annexes

Annex 1

Data Protection Rules for Project 'ICROSS'

Preamble

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 1
Definitions

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 4
Processing Sensitive Personal Data

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 5
Information To Be Given To The Data Subject

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 6
The Data Subject's Right Of Access To Data

[illegible]

The Data Subject's Right To Rectify, Erase or Block Personal Data

[illegible]

Article 8
Confidentiality And Security Of Processing

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 9
Transfer Of Personal Data To Third Countries

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 11

Storage, retention and destruction of personal data

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 11

Data Protection Officer

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Article 12
Other Provisions

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Annex

Declaration of accepting the Ethics Code including the Data Protection Rule

(for individuals and for legal entities, on separate pages)

<page intentionally left blank>

DECLARATION
on accepting the Ethics Code including the Data Protection Rule
for individuals

I, <NAME>, born in <POB> on
the <DOB> hereby declare that I have read and accept the Ethics
Code including the data protection rules of the project 'ICROSS' and I understand my rights and
obligations related to the project.

.....
<SIGNATURE>

I declare that the ICROSS Consortium processes my personal data with my consent.

.....
<SIGNATURE>

I declare that the ICROSS Consortium processes my personal sensitive data with my consent.

.....
<SIGNATURE>

(Only sign the appropriate declarations!)

.....
<DATE>

In witness whereof:

..... <NAME>
..... <ADDRESS>
..... <SIGNATURE>

..... <NAME>
..... <ADDRESS>
..... <SIGNATURE>

DECLARATION

on accepting the Ethics Code including the Data Protection Rule for legal entities

Name of Legal Entity:.....
Seat of Legal Entity:.....
Registration number:.....
VAT number:
PIC number:

represented by<NAME and POSITION>

hereby declares that the above mentioned legal entity accepts the Ethics Code including the data protection rules of the project 'ICROSS' and understands the rights and obligations related to the project.

.....
.....

<DATE>

.....

<SIGNATURE and STAMP>

DATA PROCESS REGISTER

Name of entity:

Project Name: iCROSS

Numbered list of data types processed:

Start of process period:

End of process period:

Date:

Data Protection Officer

ACCESS TABLE

Mark level in corresponding column (see numbered list above).

Access levels: O=read, I=write, X=admin

Name of person	Access	Revoke	1	2	3	4	5	6	7	8	9	10	11	12	12

(add lists as required)

DATA TRANSFER REGISTER

Transferring Entity	Recipient	Purpose of Transfer	Legal ground of Transfer	Personal Data Transferred	Time of Transfer	Other

Section 6: Security⁷⁶

Activities or results, involved in the project, raising security issues: NO

“EU-classified information” involved in the project as background or results: NO

6.1 Security aspect letter

To be provided by commission service during the Grant Agreement preparation

6.2 Security classification guide

Since the iCROSS platform will collect, analyze, and evaluate only tools that are developed within the project itself without intervening in regular operations to border control. We expect that there will be no need to classify any of the expected deliverables in terms of their security aspects. This is a research and innovation action, and special care was put in the design of iCROSS to focus on automating tasks that border control agents do that are already publically available. To better design iCROSS members of the consortium who were or are directly involved both in relevant policy as well as in border control participate in the project and any tasks of the project that may require a security classification will either be performed by them, or other partners with sufficient security clearance and relevant outcomes of those tasks will not be disseminated to anyone without adequate security clearance. As an extra risk mitigation in the unlikely event that a partner doesn't have sufficient security clearance and is crucial to a task, then that partner will apply to the process to acquire that security clearance, to facilitate this enough time has been allocated from the beginning of the project until the implementation stages to apply and receive clearance.

6.3 Security staff

6.3.1 Project Security Officer

[REDACTED]

6.3.2 Security Advisory Board

A Security Advisory Board (SAB) will be set up with representatives from the consortium and end-users with sufficient knowledge of security issues to assess the sensitivity of the following deliverables prior to publication: D2.1, D2.2, D3.1, D3.2, D3.3, D4.1, D4.2, D6.3 and D6.4. Based on the evaluation of the SAB on deliveries, the dissemination of any content assessed as sensitive will be limited to the consortium on the SABs decision. SAB is empowered to change dissemination level of deliveries to the level justified by the results incorporated (eg. from PU to CO or vice versa). The Security Advisory Board will be led by [REDACTED] who has been assigned with the role of the **Project Security Officer**; whereas representatives from ED (as coordination team), ITTI, EVR, JAS (as tech providers with great

⁷⁶ Article 37.1 of Model Grant Agreement. Before disclosing results of activities raising security issues to a third party (including affiliated entities), a beneficiary must inform the coordinator — which must request written approval from the Commission/Agency; Article 37. Activities related to ‘classified deliverables’ must comply with the ‘security requirements’ until they are declassified; Action tasks related to classified deliverables may not be subcontracted without prior explicit written approval from the Commission/Agency.; The beneficiaries must inform the coordinator — which must immediately inform the Commission/Agency - of any changes in the security context and — if necessary — request for Annex 1 to be amended (see Article 55).

expertise in the field of critical systems for security and emergency), PBG, BSG, TRAINOSE (as end-users) will constitute the Board.

6.4 Other project-specific security measures

As part of work package 2 in iCROSS the security requirements will be established based on both the national, and EU level legislation and border control procedures. Any problems identified, such as the inability of staff without personal security clearance required to access secure premises for the needs of the deployment of the Pilots for example, will be addressed by the partners responsible for each Pilot. Each Pilot will be performed by the same institutions who are responsible for the security of the areas where the Pilots will take place and the pilots themselves will include the use of real border control agents taking part in the project. Since all of them have security clearance in each of the respective Pilot execution sites, we don't anticipate any problem. The Requirements task and the legal compliance task will enable the definition of the requirements that need to be addressed so that border control agents are capable of executing the Pilots, such as user friendly technical set up procedures, stand by telephone technical support by technical experts etc.

Annex

