EUROPEAN COMMISSION
DG Migration and Home Affairs

Direction E: Migration and Security Funds: Financial Resources
Unit E4: Union Actions and Procurement

SPECIFIC CONTRACT

HOME/2019/ISFP/FW/LECO/0011

implementing framework contract No HOME/2016/FW/LECO/0001

1. The European Union ('the Union'), represented by the European Commission ('the contracting authority'), represented for the purposes of signing this specific contract by [redacted]

and

Milieu Consulting SPRL
Registration number BE0549992374
VAT BE0549992374
Chaussée de Charleroi 112
BE-1060 Brussels

("the contractor"), represented for the purposes of signing this specific contract by [redacted]

[redacted]

HAVE AGREED

ARTICLE 1 SUBJECT MATTER

1.1 This specific contract implements framework contract (FWC) No HOME/2016/FW/LECO/0001, as amended on 24/11/2016.

1.2 In accordance with the provisions set out in the FWC and in this specific contract and its annexes, which form an integral part of it, the contractor must provide the following services: "**Study on the retention of electronic communications non-content data for law enforcement purposes**".

ARTICLE 2 ENTRY INTO FORCE AND DURATION

2.1 This specific contract enters into force on the date on which the last party signs it.

2.2 The provision of the services starts from the date when specific contract enters into force.

2.3 The provision of the services must not exceed **30 weeks**. The parties may extend the duration by written agreement before it elapses and before expiry of the FWC.

ARTICLE 3 PRICE

3.1 The maximum total amount covering all services to be provided under this specific contract is [redacted].

3.2 N/A

***

In Belgium, use of this contract constitutes a request for VAT exemption No 450, Article 42, paragraph 3.3 of the VAT code (circular 2/1978), provided the invoice includes the statement: 'Exonération de la TVA, Article 42, paragraphe 3.3 du code de la TVA (circulaire 2/1978)' or an equivalent statement in the Dutch or German language.

ARTICLE 4 COMMUNICATION DETAILS

For the purpose of this specific contract, communications must be sent to the following addresses:

Contracting authority:

For all contacts with the Commission, the Contractor will use the following email address:

HOME-NOTIFICATIONS-D4@ec.europa.eu

with the following email addresses in c.c.:

[redacted]

[redacted]

and

[redacted]

Postal address:
European Commission
Directorate-General Migration and Home Affairs
Directorate D - Unit D4
Att: [redacted]
L-15 02/P079
BE-1049 Brussels

Financial matters (Reports and invoices):

European Commission
Directorate-General Migration and Home Affairs
Directorate E - Unit E4
[redacted]
LX46 04/158
BE-1049 Brussels
Email: [redacted]

Contractor:

Milieu Consulting SPRL
[redacted]
Chaussée de Charleroi 112
BE-1060 Brussels
E-mail: [redacted]

ARTICLE 5 PERFORMANCE GUARANTEE

Performance guarantee is not applicable to this specific contract.

ARTICLE 6 RETENTION MONEY GUARANTEE

Retention money guarantee is not applicable to this specific contract.

Annexes

- Request for service
- Contractor's specific tender

[redacted]

Signatures

For the contractor,

[redacted]

signature: [redacted]

Done at Brussels on 22/11/2019

For the contracting authority,

[redacted]

signature: [redacted]

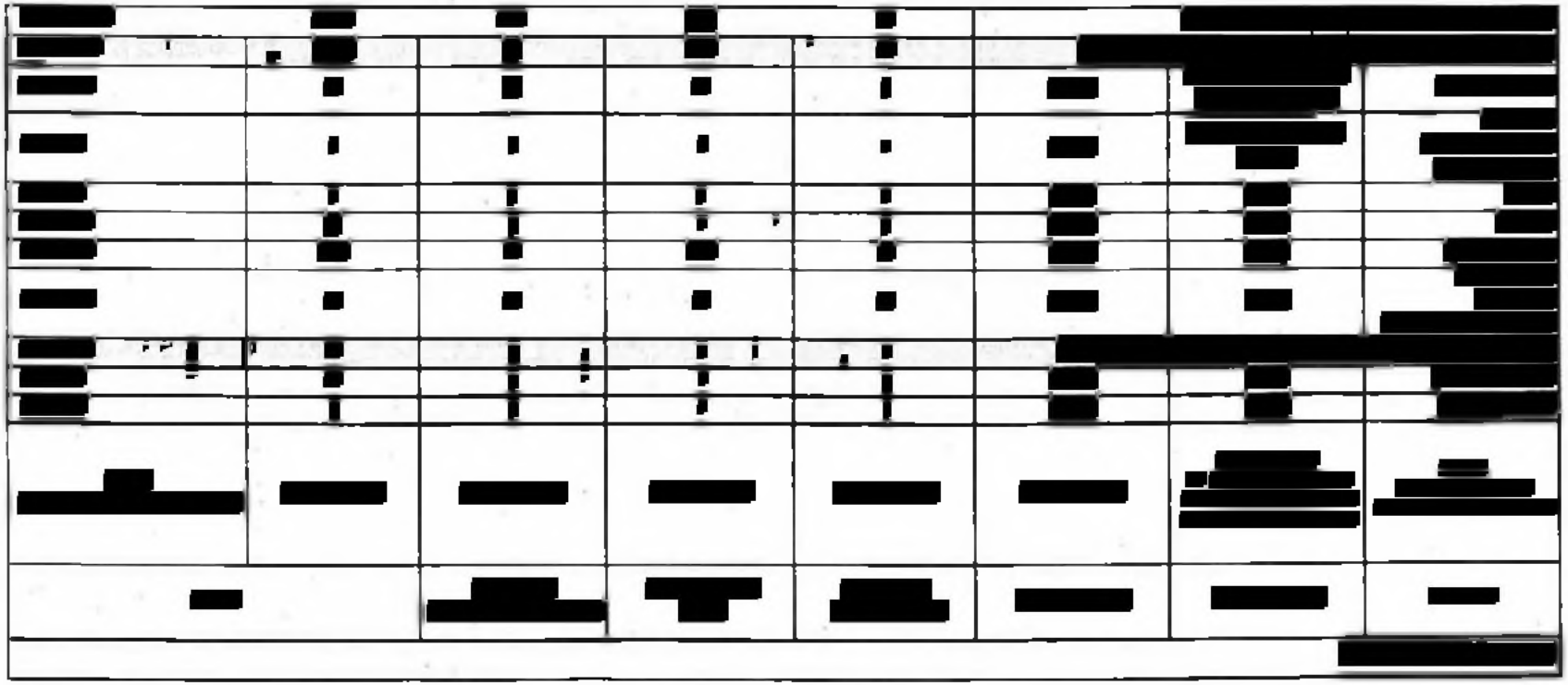
Done at Brussels, on 22/11/2019

In duplicate in English.

[redacted]

[redacted]

[redacted]



Specific contract HOME/2019/ISFP/FW/LECO/0011 under the FWC HOME/2016/FW/LECO/0001

Terms of reference

Study on the retention of electronic communications non-content data for law enforcement purposes

1. Context of the study

Electronic communications activities, occurring through traditional circuit-switched telephony or packet-switched internet transmission, generate electronic data. These data may be understood as either 'content' (e.g. the conversation during the telephone call, the message in the email) or 'non-content' data[1]. Non content data (also known as 'metadata') include information on the identity of subscribers or clients (i.e. service-associated information e.g. telephone numbers, IP addresses), traffic (i.e. communication-associated information e.g. logs of calls received and made or logs of messages exchanged), and location of the user at the time of the communication. Providers of publicly-available electronic communications services and/or of electronic communication networks (henceforth referred to as 'operators') store or log such non-content data, usually for few months at most, for business or commercial purposes including billing and interconnection payments (which enable differential pricing), and related fraud detection and prevention, marketing or the provision of value-added services to the extent and as long as they are allowed to do so in accordance with the national law and the ePrivacy Directive[2].

Just as communication technology use has increased in the past years, criminals also make extensive use of it for many different purposes. Where eye witness accounts or confessions and other forensic evidence are unavailable, historical non-content data can be the main lead to identify a suspect or to identify his/her accomplices at the start of an investigation, and to decide whether it is justified to use more intrusive surveillance tools, like interception. These data are particularly valuable in cases (a) where internet/telecommunication services are used to plan, prepare and/or commit a crime, (b) involving complex organised crime structures, (c) of uploading/downloading child pornography, and (d) of identity theft or using false identities. Where such data are not available, there may be limited possibility to investigate or prosecute the case or alternative and more costly approaches may be required to complete the investigation.

---

[1] For definitions see Directive 2002/21/EC and ETSI Technical Standard 101 331.

[2] Directive 2002/58/EC as amended by Directive 2009/136/EC. For instance, Article 6(2) ePrivacy Directive allows operators to process traffic data necessary for the purposes of subscriber billing and interconnection payments. For other purposes, operators need to obtain users' consent. Furthermore, for matters not specifically addressed in the ePrivacy Directive, such as users' data protection rights, operators need to comply with the general data protection rules contained in the General Data Protection Regulation (GDPR - Regulation (EU) 2016/679).

Police and judicial (henceforth referred to as 'law enforcement') authorities tend to rely on forensic analysis of communications non-content data in detecting and investigating and prosecuting threats to public security and maintaining law and order. They argue that, in order to maintain a sufficient level of operational capability, it is necessary to ensure the availability of non-content data generated by the use of electronic communications. Consequently, since early 2000s, some EU Member States have introduced compulsory retention of electronic communications non-content data (subscriber, traffic and location data) for law enforcement purposes.

At the EU level, Article 15(1) of the 'e-Privacy Directive' (Directive 2002/58/EC), provides for the possibility for Member States to impose on providers the obligation to retain electronic communications data for a range of public interest purposes. Aside from this possibility, the e-Privacy Directive requires providers to erase or made anonymous the data after the transmission of the communication or, by derogation, as soon as it is no longer required for business purposes, such as billing. Regarding location data, its processing by providers is subject to the consent of the users. Directive 2006/24/EC, known as the Data Retention Directive (DRD) provided for compulsory retention of electronic communications non-content data for law enforcement purposes and harmonised certain aspects of data retention in the EU.

Whereas the e-Privacy Directive provides for the possibility to retain certain data for a limited period for the purposes listed in Article 15(1) thereof, the DRD created the obligation to retain these data, for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The DRD did not relate to how data would be accessed and used by competent law enforcement authorities.

The Court of Justice of the European Union (CJEU) declared the DRD invalid on 8 April 2014, following two requests for a preliminary ruling (cases C-293/12 *Digital Rights Ireland* and C-594/12 *Seitlinger et al*). The Court held, inter alia, that Directive 2006/24 entailed a wide-ranging and particularly serious interference with the fundamental rights to privacy and data protection as laid down in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary. It also held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter. After this judgment, Member States that kept in place laws obliging telecommunications service providers to retain (non-content) communications data for a specified period for criminal law enforcement purposes did so directly based on Article 15(1) of the e-Privacy Directive.

[redacted]

In the subsequent *Tele2 and Watson*[3] judgment of 21 December 2016, the CJEU concluded that Article 15(1) of the e-Privacy Directive[4], read in the light of the Charter of Fundamental Rights, precludes national legislation which:

- for the purpose of fighting crime, *"provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication"*,
- in the context of fighting crime, does not restrict access of the competent national authorities to the retained data *"solely to fighting serious crime"*,
- does not subject such access *"to prior review by a court or an independent administrative authority"* and
- does not require that the data concerned be retained within the European Union.

On 10 January 2017, the Commission tabled a proposal for a new e Privacy Regulation[5] to replace and update the current e Privacy Directive, including by expanding the scope to cover not only traditional telecommunication services but also so called Over the-Top communications services (OTTs). The relevant scope of the derogation permitted under Article 11(1) of the proposed e Privacy Regulation is essentially the same as that under Article 15(1) of the current e-Privacy Directive.

The Court does not intrinsically prohibit data retention schemes nor does it confine Member States solely to establishing a data preservation system (so called 'quick freeze'). However, the Court seems to exclude "*general and indiscriminate retention*" of all traffic and location data. It would accept retention schemes that are restricted in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime. There has been uncertainty on how to implement those criteria.

The invalidation of the Data Retention Directive and subsequent decisions of the CJEU have fuelled a degree of uncertainty amongst a broad range of actors (Member States, law enforcement and judicial authorities, communication service providers and citizens). This is due to a number of reasons: the uneven patchwork of existing data retention regimes in different Member States, the different stages of and approaches to legislative revisions that some Member States are undergoing, the various legal challenges to national laws, etc.

---

3 Judgment of the Court of Justice of the EU (Grand Chamber) *"Tele2 and Watson"* of 21 December 2016 in joined Cases C-203/15 and C-698/15, operative part. The judgment stems from two references for a preliminary ruling from Sweden and the UK in relation to the data retention obligations imposed on service providers under the national laws of those two Member States.

4 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 201, 31.7.2002, p. 37).

5 COM(2017) 10 final. The draft proposal is currently under consideration by the European Parliament and the Council under the ordinary legislative procedure.

Following the abovementioned Court rulings, the situation in the EU has evolved in the direction of increasing diversity of the national data retention systems:

- There is no longer a harmonised data retention system in the EU due to the invalidation of the Data Retention Directive in 2014.

- Following the 2014 *Digital Rights* and the 2016 *Tele2* rulings, Member States' laws implementing the DRD were either amended, left unchanged or struck down by the national (usually constitutional) courts and either subsequently amended or not renewed at all.

- In some Member States data retention laws are not in force (NL, SK, SI, AT) or are being revised (SE) or the law is in place but not being enforced after judicial suspension (DE).

- Data retention laws are subject to national court challenges brought by civil society groups, professional associations or telecommunication operators on the grounds of incompatibility with Union law, including the Charter of Fundamental Rights as interpreted by the CJEU (e.g. DE, FR, BE, DK).

- Requests for preliminary rulings are pending at the CJEU (from UK, BE, FR, EE) seeking clarity on various points of the rulings and their impact on national data retention legislation in both the law enforcement and national security contexts.

Both the Commission and the Council, with support from Europol and Eurojust, have been engaged in a common reflection process on data retention for the purposes of the prevention and prosecution of crime in the light of the Court judgments. This ongoing process has mainly focused on ensuring the availability of data for law enforcement authorities, possible ways of restricting the scope of existing data retention systems and setting access safeguards.

In the context of this reflection process, on the 6 June 2019, the Council adopted the *Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime.*[6]

In these Conclusions, the Council requested the Commission *inter alia* to prepare a comprehensive study on possible solutions for retaining data. Such study should also take into account:

• the consultations with the relevant stakeholders

• the evolving case-law of the Court of Justice and of national courts relevant for data retention; and

[6] https://data.consilium.europa.eu/doc/document/ST-10083-2019-INIT/en/pdf

[redacted]

- the outcomes of the common reflection process in the Council;

The present study is a contribution to the comprehensive study requested by the Council to the Commission.

2. Objective of the study

The general objective of the study is to support the Commission with an independent evidence-based analysis of the current situation regarding retention and access to non-content electronic communications data for law enforcement purposes in selected Member States.

The aim is to provide useful input for assessing whether and under which conditions data retention rules and practices are fit for purpose taking into account the general objectives of effectively preventing, investigating and prosecuting criminal offences.

More specifically the study should:

a. provide a comprehensive overview of existing legal rules and practical arrangements concerning retention and access to non-content communication data for law enforcement purposes,

b. identify the categories of data and data storage practices of the telecommunication industry regarding non-content data stored for commercial purposes,

c. identify specific needs of the law enforcement authorities regarding access to different categories of non-content data and to collect relevant evidence (qualitative and quantitative) to justify these needs, ideally through statistics and concrete, illustrative case-studies

d. identify relevant technological challenges to existing arrangements regarding retention and access to non-content data (e.g. use of dynamic IP addresses, impact of introduction of 5G, encryption) and to describe the projected measures, if any, to address such challenges, including their implications with regard to the existing legislative framework and costs.

The objective of the study is not to propose legal drafting suggestions or to evaluate the compliance of the national legislation with EU law.

The findings will serve as input for the Commission to draw policy conclusions and feed into possible consideration on the future of the relevant regulatory framework.

3. Scope of the study

The study will cover a sample of ten (10) selected EU Member States: Austria, Estonia, France, Germany, Ireland, Italy, Poland, Portugal, Slovenia, Spain. These Member States are selected due to their different legislative and practical approaches to the data retention obligations.

The study should provide empirical data for the period 01.01.2018-31.08.2019. However if such data are not yet available, data for a most recent period of 1 year are acceptable.

The Contractor should consult all key stakeholders in the course of the study, including but not limited to:

a. Representatives from law enforcement competent authorities involved in access and use of the non-content data for law enforcement purposes

b. Representatives from telecommunication operators and internet service providers, including those providing OTT services, which are concerned by the retention and access to non-content data for law enforcement purposes

c. Representatives from the telecom regulatory authorities

d. EU staff in DG HOME, DG JUST, DG CNECT, Europol, Eurojust, and other EU services if relevant.

4. Description of the tasks

The task consists of the production of a retrospective fact finding support study from an inter-disciplinary perspective, i.e. legal perspective, telecommunication industry perspective, law enforcement operational perspective, technological perspective.

The study shall provide useful input and data for answering the specific questions identified below. Then, comprehensive answers to the questions below should be provided for each of the 10 selected Member States.

The formulation of the questions listed below can be subject to slight modifications by the Commission during the inception stage of the process.

4.1. Legal framework

- What is the national legal framework regarding the retention of non-content data (hereafter "data") for law enforcement purposes? Is there any specific legal obligation to retain data for law enforcement purposes? What are these obligations (who has to retain what and for how long)?
- What is the national legal framework regarding the access to non-content data by the law enforcement authorities (who can request and ex-ante authorise access, for what purposes, is there any ex-post control, what data can be accessed, etc.).
- Are there any legal and/or political challenges to relevant national legal framework? What is their scope? Are there any ongoing processes aiming at amending the legislation?

4.2. National practices

- What non-content data are retained and for how long by the telecommunication industry and other relevant service providers? Are they retained for commercial/business purposes and/or for law enforcement purposes? What data is retained solely due to the obligation of retention for law enforcement purposes and would therefore not be retained for commercial/business purposes?

- What are the additional costs associated with retention of data for law enforcement purposes? Are these costs reimbursed to the industry?
- What is the impact of the retention and access to data for law enforcement purposes on the business models of the telecommunication industry?
- What is the number of requests for a given time period according to the category of data requested e.g. subscriber fixed and mobile telephony data (who registered a phone number), traffic data (who called whom and at what time), location data, other metadata (such as computer metadata, IP addresses, IP logs etc.)?
- What are the proportions of requests according to the types of providers: telephony companies, internet service providers, OTTs, etc.? What percentage of requests are national or cross-border?
- What is the volume of data requested? In particular, how common are the requests to data sets related to a large number of persons? Do the requests usually target specific individuals (suspects) or rather larger groups of people e.g. all telephone users who used their phones in a specific perimeter/geographical area where a crime took place?
- What is the average "age" of the requested data? How far back in time do the requests usually go? What is the proportion of requests for data generated less than 1 month, 3 months, 6 months, 1 year ago?
- What is the proportion of the requests which are refused? What are the reasons of such refusals?
- For what purposes have data been requested (e.g. prevention of crime, investigation of crime, civil claims)? What are the proportions of requests for different purposes (e.g. different types of crime)?
- How is the proportionality and necessity assessed in practice while the request in made/authorised?
- What are the alternatives available to requesting the data (e.g. data preservation/quick freeze, non-digital evidentiary alternatives)?
- How the process of requesting and accessing the data works in practice? What is the procedure to follow? How long it takes to receive the data? What are the practical arrangements (forms, points of contact, etc.)?
- What is the procedure to request data from other jurisdictions (other Member States or third countries)?
- In case a retention regime limited to some geographical areas, some specific persons and/or some specific categories of data would be implemented, what data should be retained as a matter of priority? Who and how should conduct the risk/threat assessment to establish the relevant targets?

4.3. Benefit of using the data

- What is the quantitative proportion of cases in which non-content telecommunications data are used in criminal investigations and prosecutions as compared to all investigations and prosecutions?

Among these what is the proportion of cases in which non-content communication data were used as determinative and/or exclusionary evidence in the course of the investigation i.e. to identify/eliminate suspects, accomplices, victims, witnesses, alibis etc.? What are the typical case examples? Is it possible to determine whether data used in such cases are originally retained by the telecommunication industry for commercial/business purposes or for law enforcement purposes?

What is the number of cases that could not be investigated because of the absence of non-content communications data held by providers? What are the reasons e.g. provider which holds the data cannot be identified; provider can be identified, but it is located in another jurisdiction; data were not stored and/or already deleted by the provider; data exists but are encrypted? What are the typical case examples?

- How the absence of communications non-content data affects the general efficiency and effectiveness of criminal investigations and prosecutions. What alternative investigative techniques are available?
- Are the communications metadata non-content data used for the purpose of preventing crime? What is the benefit of such use of data?

4.4. Technological context

- What is the impact of encryption on access to non-content communication data for law enforcement purposes?
- What is the impact of the new standards or new technologies (e.g. 5G) on retention and access to non-content communication data for law enforcement purposes?
- What are the measures (if any) which are envisaged to ensure access to non-content communication data for law enforcement purposes in the context of such technological changes?

Based on the answers to these questions, the Contractor will formulate clear, robust and evidence-based conclusions.

5. Data collection and methodological approach

In performing the study requested under section 4, the contractor will carry out the following tasks:

Task 1: [Definition of methodology]: The contractor will identify in the inception report the methodology to collect information, analyse and assess questions listed in section 4, the indicators and information sources – quantitative and qualitative – that allow answering the questions. A detailed description of the methodology, the respective advantages, limitations and risks involved in using the proposed methodology should be included, as well as the strategies the contractor intends to use to mitigate the risks identified with the different information sources. There must be a clear link between the question addressed and the corresponding methodology proposed.

Task 2: [Quantitative data]: The contractor will identify, collect and process the publicly available information and data to perform the requested service. The data collection activities shall be agreed with the Commission at the inception stage before their launch. All data collected for the study shall be made available to the Commission.

Task 3: [Collection of qualitative and qualitative data via consultation of a target group]: In order to collect the data requested under the questions listed in section 4, the contractor shall conduct a targeted stakeholder consultation via a mix of surveys and targeted interviews. The survey shall cover a representative sample of relevant stakeholders, in particular law enforcement authorities and telecommunication service providers. The identification of the relevant shareholders might differ depending on the question concerned. The list of the relevant stakeholders for both surveys and interviews will be agreed with the Commission. The questionnaires need to be drafted in the language of the Member States in which the consulted stakeholders are located. The questionnaires need to be transmitted to the Commission for approval in T0 + 4 weeks. There must be a clear link between the questionnaires and the information and data that they aim at collecting. If the results of the questionnaires are inconclusive (e.g. low response rate, lack of and/or conflicting data), the contractor will take necessary additional steps to draw clear conclusions and will ensure a representative sample of the opinions of relevant stakeholders. In particular, this may take the form of a series of follow-up interviews with relevant stakeholders (complementary to the general interview program). The contractor shall reach a level of at least 50 % response rate to survey questionnaires (i.e. 50% of the consulted stakeholders must have replied to each of the surveys). The contractor will at the latest two working days after the deadline to reply to the questionnaire concerned inform the Commission if the response rate to one of the surveys is not reached and inform the Commission of the strategies proposed to increase the response rate. The contractor shall implement those strategies with a view to increase the response rate after validation by the Commission of the strategy. Regarding the targeted interviews, the contractor should interview at least 6 different stakeholders in every of 10 Member States within the scope of the study. All the categories of stakeholders listed under a., b. and c. in point 3 should be represented in each Member State.

6. Deliverables and reporting

6.1. Deliverables

The contractor must ensure that all deliverables under the contract are clear, concise and comprehensive. Reports must be drafted in English, unless otherwise specified, using simple and non-technical language for a non-specialised audience. Technical explanations shall be given in annexes. All relevant evidence of the analysis process (e.g. questionnaires, results of surveys and interviews) has to be annexed to the report to allow the argument to be followed in a transparent manner and the results to be replicated. The contractor will also present the analysis of the quantitative data in the form of relevant tables and graphs. Excel sheets including formulas for any calculations carried out by the consultants to support tables or graphs in the study must also be provided.

The contractor is requested to deliver:

1) An inception report for reviewing must specify the detailed work programme and planning of the study in order to complete all the tasks as listed in section 4 of the technical specifications. It will describe the proposed methodological and empirical approaches and working assumptions. The report will also contain a risk assessment relating to information gathering and include the mitigation strategies proposed to reduce the risk of not obtaining the expected data or information (in particular in the framework of surveys and interviews). The report will also identify any additional need for information to be collected and present data collection methodology and tools applied to select the contacts to be surveyed. A detailed work plan including the allocation of experts per task per number of working-days must also be provided. It should not exceed 45 pages (annexes excluded).

2) The survey and interviews questionnaires to be developed to obtain the data requested under the section 4 above.

If the contracting authority has observations to make, it must send them to the contractor and suspend the time limit for payment in accordance with Article II.21.7. The contractor (or leader in case of a joint tender) has 20 days to submit additional information or corrections or a new version of the documents if the contracting authority requires it.

3) An interim report for reviewing must summarise the results of the information and data collection phase. It must include the initial results of the desk research and survey and an assessment of the quality of the data received, and must present the preliminary findings of the evaluation questions. It must also provide an update of the process, activities carried out, problems encountered, solutions applied and a detailed planning of the work to be carried out during the remaining contract duration. It must flag any changes in the initially planned methodology, specify the status of any findings/conclusions/suggestions for follow-up and raise any problems encountered with sufficient information to permit reorientation, if appropriate. It will also include the structure of the final report for the approval by the Commission. The contractor has 20 days to submit additional information or corrections or a new version of the interim report for acceptance.

The executive summary of the interim report will provide an overview and orientation of the report and outline the preliminary conclusions.

5) A final draft report for reviewing must cover all tasks and take account of the comments made earlier by the Commission in the process. It must provide answers to all evaluation questions based on sound analysis of findings. It must present factually based preliminary conclusions and suggestions for follow-up, in line with the description of tasks in section 4. In particular, it must provide a summary of the results of the targeted stakeholder consultation. Overall it should not exceed 90 pages (annexes excluded). Only in duly justified circumstances, the final report could exceed 90 pages (annexes excluded) subject to prior consultation of the contractor with the Commission.

Given that the study may rely on some data that is covered by rules on professional secrecy, the contractor will be required to produce the draft final report and most of the annexes in a publishable way, only containing non-confidential information.

All confidential information must be concentrated in one or two confidential annexes that will be provided to the Commission but will not be published.

The contractor will make it clear in all requests to stakeholders that its request should be treated in full respect of data protection rules, which may require transmission of anonymised data only.

6) A final report for acceptance follows in principle the same structure as the draft final report while taking into account Commission's comments and requests, as relevant.

The contractor will draft the main final report and annexes in a publishable way, only containing non-confidential information. All confidential information must be concentrated in one or two confidential annexes that will be provided to the Commission but will not be published.

The Commission may decide to publish the non-confidential version of the Final Report, the Executive Summary, the Abstract and the non-confidential Annexes on the Internet.

7) A publishable executive summary of the final report (maximum six pages) and an abstract (maximum 200 words) must be provided in English. This should be accompanied by a PowerPoint presentation in English also summarising the final report.

6.2. Meetings and reporting

The contractor is expected to be present in Brussels at the premises of the Commission at a kick off meeting, at a meeting to present the inception report, the interim report and at another meeting when the draft final report will be presented.

The data collection activities will have to be presented in a meeting in Brussels at the premises of the Commission before they are launched. For each meeting the contractor will prepare a PowerPoint presentation. All other meetings will be organised via conference calls.

Following each meeting, the contractor will draft minutes and agree them with the Commission within 5 working days after meeting.

Once every 2 weeks throughout the whole period of the study the contractor will provide the Commission with a short progress report. Reports shall discuss the key progress and state of play of the study, the main problematic issues faced by the contactor and further steps. The format of the progress reports will be agreed at the kick-off meeting.

The Contractor is expected to assist the Commission in presenting the progress of the study during the duration of the Contract to the relevant Council working party delegates (DAPIX). This includes one presentation of the interim or final report in Brussels. The exact date will be determined according to the Commission and Council work programmes.

7. Confidentiality and intellectual property rights

The requirements under section 3.3 of Annex I (Tender Specifications) of the Framework contract are applicable.

All information and data provided under this specific contract are deemed confidential, unless those are already in public domain.

The contractor agrees to treat any documents to which access is granted by the Commission in the context of this contract as being confidential. This includes any correspondence between the Commission and the contractor.

All data collected by the Contractor and the various reports are the property of the European Commission. Rights relating to its reproduction and publication will remain the property of the European Commission. No document based, in whole or in part, upon the work undertaken in the context of this contract may be published without the prior formal written consent of the European Commission.

8. Starting date and duration of tasks

The duration of the tasks shall not exceed 30 weeks.

Execution of the tasks begins on the date on which the specific contract is signed by the last signing party.

The contractor is deemed solely responsible for delays occasioned by sub-contractors or other third parties (except for rare cases of force majeure). Adequate resources and appropriate organisation of the work including management of potential delays should be put in place in order to observe the timetable.

The following outline work plan and indicative timetable are envisaged. However, the contractor is expected to respect the final deadline.

Deadline	**Task**
T0 (Signature)	
T0 + (1) week	**A kick-off meeting** will be held on the Commission premises within one (1) week of the contract being signed. The kick-off meeting will ensure that the contractor has a clear understanding of the terms of the contract and the objectives of the project. The contractor will be provided with relevant available documents and be informed of useful information sources for data collection. This will be an opportunity to raise initial issues regarding the proposed analytical framework, methodology and overarching data collection strategy, but also to agree on the draft structure of the Inception, Interim and Final Reports. The Contractor should submit draft structures for these reports as part of the offer.
T0 + (4) weeks	Within four (4) weeks of the contract being signed, the Contractor will submit an **Inception Report** for review. This report will specify the analytical framework, methodology and overarching data collection strategy, including specific tools that the Contractor intends to utilise in carrying out the study. This will include **questionnaires for use in carrying out any interviews/surveys** that are required as part of the

	study. Drafts of any such tools should be provided at this time. The Inception Report for review will also include a detailed work plan.
T0 + (5) weeks	A **meeting** will be held between the Commission and the Contractor on the Commission's premises within one (1) week of the submission of the Inception Report for review. The purpose of this meeting is to provide comments on the Inception Report for review and any other relevant aspects of the Contractor's work, including the mapping of available data and questionnaires for use in carrying out any interviews/surveys.
T0 + (6) weeks	The Inception Report for acceptance will be submitted by the Contractor to the Commission within one (1) week of Inception Report meeting.
T0 + (15) weeks	The contractor submits the **interim report.** Within 2 weeks the report will be discussed in a meeting with the Commission in Brussels. If necessary, the contractor will revise the report and the amended interim report will be sent to the Commission within 20 days from the receipt of the Commission comments
T0 + (26) weeks	The contractor submits the **draft final report**. Within 2 weeks the report will be discussed in a meeting with the Commission in Brussels.
T0 + (30) weeks	The contractor submits **the final report**, which reflects the comments of the Commission publishable executive summary of the final report and an abstract. The Final Report should be provided by the Contractor in six (6) hard copies and digitally (both in MS Word and PDF formats). The Final Report shall adhere to the same structure as the Commission's Staff Working Documents the Commission's "visual identity" policy as articulated in the Commission's Visual Identity Manual.[7]

9. Contact details

For all contacts with the Commission, the Contractor will use the following email address:

HOME-NOTIFICATIONS-D4@ec.europa.eu

with the following email addresses in CC:

[redacted]

[redacted]

[7] This document is available at the following web address: https://ec.europa.eu/info/sites/info/files/charter_en_0.pdf

[redacted]

10. Estimated volume of the contract

The estimated volume of work for the required service, covering all the tasks and deliverables as listed above is approximately 150 working days for the total contract duration. The contractor will submit a breakdown of the working days per task involved.

11. Content of the offer

The offer must be in conformity with the provisions of the Framework contract and must include:

1. A technical part as further detailed in the technical specifications, including:

a) a detailed description of the proposed approach, methodologies and information sources to be used as well as the suggested structure of the report;

b) the composition of the team and organisation of the work within the team.

2. A financial part in the form of a global price ("all inclusive" offer).

The global price shall be broken down and presented in the form of a table as follows:

- the daily rate respecting the price per expert-person-day fixed in the Framework contract;
- the total number of person-days that each expert will contribute to the project;
- the total price (= expert-person-day price multiplied by total of expert person-days).

3. An administrative part, including a declaration on honour to attest the absence of conflict of interest and a declaration on confidentiality, to be signed by each expert.

The bidder should provide a list of identified risks and constraints that he foresees in carrying out the study. This should be accompanied by a mitigation plan describing how the bidder intends to cope with these risks/constraints.

The management of sensitive information should be thoroughly addressed as part of the data collection strategy described in the bit submitted to the Commission. In the offer, the bidder should explain how he intends to receive, store, exploit, and then - at the conclusion of the evaluation - destroy sensitive data using an appropriate and certified information management system.

12. Expertise

The Project Manager should have at least five years' demonstrable experience in managing projects on this scale (timeframe and budget).

The team carrying out the study should have expertise in legal and economic analysis. The team should possess a good knowledge of current issues in the area law enforcement and telecommunication technology.

One member of the team should have at least seven years' experience in collecting and evaluating evidence in a policymaking context, including developing and using quantitative indicators.

Two further members of the team should have at least three years' experience in collecting and evaluating evidence in a policymaking context.

At least one member of the team should have an excellent command of written English.

13. Budget

The maximum available budget for this study i[redacted]

[redacted]