



Request for Tender: Forensic Software

Issue/Publication Date: 10/09/2025



1. Contents

1.	INTRODUCTION	3
2.	TENDER INFORMATION	4
3.	SPECIFICATION OF REQUIREMENTS – LOT 1 (ANDROID)	5
4.	SPECIFICATION OF REQUIREMENTS – LOT 2 (IOS)	6
5.	SPECIFICATION OF REQUIREMENTS - LOT 3(COMPUTER BASED DEVICES)	7
6.	ESSENTIAL QUALIFICATION REQUIREMENTS	8
7.	SELECTION CRITERIA	8
8.	AWARD CRITERIA	8
9.	EVALUATION	9
10.	FURTHER INFORMATION	10
11.	SUBMISSION	12



1 Introduction

1.1 The Office for the Police Ombudsman (Fiosrú) is an independent statutory law enforcement body established under the Policing, Security and Community Safety Act 2024. Fiosrú is responsible for receiving and dealing with all complaints made by members of the public concerning the conduct of members of the Garda Síochána.

1.2 Fiosrú headquarters are in Dublin with remote offices in Longford and Cork.

1.3 Fiosrú intends to establish two lots for the provision under two strands of Forensic Software, namely:

- Lot 1 – Android Devices,
- Lot 2 – iOS devices, and
- Lot 3 – Computer based devices

for use in the course of its investigations and statutory duties.

1.4 Below is a brief summary of part of Fiosrú infrastructure aligned to Digital Forensics to assist you in the formulation of your submission:

- All client machines are laptops running Windows 11 based on either Dell Precision Workstation 7780 (Intel i9-13950HX, 32GB RAM, Nvidia RTX 3500 Ada 12GB) or Dell Alienware m16 (Intel i9-13950HX, 64GB RAM, Nvidia RTX 3080ti)
- All client machines are running Windows 11
- All client machines have access to a dedicated internet connection and LAN/WAN capabilities

1.5 Throughout this agreement, Fiosrú intends to establish a single supplier contract for each Lot identified in 1.3 above hereafter referred to as 'the Agreement' for the duration of one (1) year. Lot 1 will commence in December 2025 and Lots 2 and 3 will commence in May 2026. Fiosrú reserves the option to extend the contract(s) by a further one (1) year subject to a successful service review with a maximum of three (3) such extensions.



2. TENDER INFORMATION

2.1 In order to be considered for appointment, tenderers must submit a valid tender which meets the minimum Qualification Criteria as set out in Section 5. Each tenderer, by submitting its tender, acknowledges and agrees to be bound fully by this Invitation to Tender.

2.2 Award of the contract will be determined on the basis of the Most Economically Advantageous Tender (MEAT) as evaluated against the Award Criteria and weightings set out.

2.3 The prices quoted will remain fixed for acceptance for the period of 90 days.

2.4 Tender submission should include:

- Capability Matrix of Supported Devices
- Costing per license / usage
- Details of production accreditation and training available including costings per staff member for recommended routes

all information necessary in order to enable Fiosrú to apply the Award Criteria set out. Fiosrú will award the contract under the requirements of the applicable European and National Procurement Legislation and Directives.

2.5 Fiosrú reserves the right;

- To reject any, or all, of the tenders received.
- Not to furnish a tenderer with additional information.
- To abandon the competition in its entirety.
- To extend any time limit set out in this invitation to tender, or waive a requirement which, in the opinion of FIOSRÚ, is minor, procedural or is not material.



3. Specification of Requirements – LOT 1 (Android)

- 3.1** The software should be at least compatible with the Fiosrú environment as set out in section 1.4. and preferably operate an optimal level within it. Where it does not operate an optimal level, tenderers must outline the recommended requirements for the proposed software.
- 3.2** The software should have a capability to download Full File System or Logical data from current commercial android mobile electronic devices based on the Android Operating System such as the Samsung S.24 Ultra in a forensically sound manner on a Consent based workflow. Advanced functions should be available on a limited basis (<30 per year with the option to buy more)
- 3.3** The software should be capable to allow investigators to image devices and store the image in a manner that demonstrates the data has not been altered in any way. The system must support attached storage.
- 3.4** The software should allow for the data to be examined and provide the ability to fully audit the examination. This includes defining access to specific elements of the data if needs be, for example a particular date range or individual application.
- 3.5** Elements such as secure storage, access control and collateral intrusion are all addressed in an investigation strategy. This software needs to be able to allow the necessary discrimination to meet the strategy of each case.
- 3.6** The software should allow for any upgrades as mobile device technology evolves and to provide necessary hardware and accessories to meet the variety of devices on the market. The tender application should outline the upgrade and support process.
- 3.7** The products from and operation of the software (current or directly prior version) has previously been accepted into evidence in common law jurisdictions.
- 3.8** The Software must be capable of providing the following functionality:
- extract and decrypt digital information from a wide range of commercial mobile devices; allow for the extraction of specific data only;
 - offer a selection of data presentation, analytical and reporting options, including exporting data to common office software applications;
 - deliver outputs that are intuitive and easy for investigators to understand and navigate; and provide access, storage and processing controls.



4. Specification of Requirements – LOT 2 (iOS)

- 4.1** The software should be at least compatible with the Fiosrú environment as set out in section 1.4. and preferably operate an optimal level within it. Where it does not operate an optimal level, tenderers must outline the recommended requirements for the proposed software.
- 4.2** The software should have a capability to download Full File System or Logical data from commercial Apple mobile electronic devices such as the iPhone 16 in a forensically sound manner on a Consent based workflow. Advanced functions should be available on a limited basis (<30 per year with the option to buy more).
- 4.3** The software should be capable to allow investigators to image devices and store the image in a manner that demonstrates the data has not been altered in any way. The system must support attached storage.
- 4.4** The software should allow for the data to be examined and provide the ability to fully audit the examination. This includes defining access to specific elements of the data if needs be, for example a particular date range or individual application.
- 4.5** Elements such as secure storage, access control and collateral intrusion are all addressed in an investigation strategy. This software needs to be able to allow the necessary discrimination to meet the strategy of each case.
- 4.6** The software should allow for any upgrades as mobile device technology evolves and to provide necessary hardware and accessories to meet the variety of devices on the market. The tender application should outline the upgrade and support process
- 4.7** The products from and operation of the software (current or directly prior version) has previously been accepted into evidence in common law jurisdictions.
- 4.8** The Software must be capable of providing the following functionality:
- extract and decrypt digital information from a wide range of commercial mobile devices; allow for the extraction of specific data only;
 - offer a selection of data presentation, analytical and reporting options, including exporting data to common office software applications;
 - deliver outputs that are intuitive and easy for investigators to understand and navigate; and provide access, storage and processing controls.



5. Specification of Requirements – LOT 3 (Computer based devices)

- 5.1** The software should be at least compatible with the Fiosrú environment as set out in section 1.4. and preferably operate an optimal level within it. Where it does not operate an optimal level, tenderers must outline the recommended requirements for the proposed software.
- 5.2** The software should have a capability to examine current standards of forensic images (E01, dd, raw) of both PC and Mac based devices, running any of the major operating systems (Windows, Linux, Mac) in a forensically sound manner.
- 5.3** The software should have a capability to conduct Cyber examinations in terms of OSINT and web related data capture and analysis.
- 5.4** The software should be capable to allow investigators to image devices and store the image in a manner that demonstrates the data has not been altered in any way. The system must support attached storage.
- 5.5** The software should allow for the data to be examined and provide the ability to fully audit the examination. This includes defining access to specific elements of the data if needs be, for example a particular date range or individual application.
- 5.6** Elements such as secure storage, access control and collateral intrusion are all addressed in an investigation strategy. This software needs to be able to allow the necessary discrimination to meet the strategy of each case.
- 5.7** The software should allow for any upgrades as technology evolves and to provide necessary hardware and accessories to meet the variety of devices on the market. The tender application should outline the upgrade and support process.
- 5.8** The products from and operation of the software (current or directly prior version) has previously been accepted into evidence in common law jurisdictions.
- 5.9** The Software must be capable of providing the following functionality:
- extract and decrypt digital information from a wide range of devices; allow for the extraction of specific data only;
 - offer a selection of data presentation, analytical and reporting options, including exporting data to common office software applications;
 - deliver outputs that are intuitive and easy for investigators to understand and navigate; and provide access, storage and processing controls.



6. ESSENTIAL QUALIFICATION REQUIREMENTS

Only those tenderers who demonstrate that they meet the stated levels of economic, financial and technical capacity will be considered. In order to enable the Fiosrú to ascertain tenderers' economic, financial and technical capacity, all tenders must address the following eligibility criteria in full. These criteria will be assessed on a pass / fail basis. Failure to comply with any rule and fulfil the criterion will result in the tenderer's elimination from the competition. All submissions must include:

- A valid tax clearance certificate.
- Insurance Details (Public Liability, Employers Liability and Professional Indemnity)
- Declaration of Bona Fides
- Technical specification on addressing the requirements of the specific lot applied
- Submissions received without the information requested above will not be considered for Evaluation and Contract Award.
- If the application is from a consortium/joint venture/grouping please provide the information requested for all parties.

7. SELECTION CRITERIA

Tenderers must demonstrate that they have delivered three contracts of a similar nature and scale (<500 devices per year) to the Fiosrú requirements under this tender during the previous three years. Please provide evidence of your previous experience in this area by completing the tables in the Response Document pages 4 to 6.

8. AWARD CRITERIA

Tenders which successfully proceed to evaluation stage will be evaluated on the following criteria:

8.1 SUITABILITY OF PROPOSED SOFTWARE

8.1.1 Thirty five percent (35%) of the total marks available are allocated to Suitability of Proposed Software. Technical ability to fulfil all details as set out in the Specification of Requirements (Section 3).

8.1.2 Ease of use, including user friendliness of the product.

8.2 SERVICE DELIVERY METHODOLOGY AND SUPPORT

8.2.1 Twenty five percent (25%) of the total marks available are allocated to Service Delivery Methodology and Support. Fiosrú requires a response time for delivery and installation of software at Fiosrú's Head Office in 150 Upper Abbey Street Dublin 1, D01 FT73.

8.2.2 After sales service and technical support:

- Proposed lead time and delivery plan (plan of engagement as specified in Section 3)



- Installation support
- Training (type, duration, location, cost)
- Number of hours training or support included in the license fee
- Post-installation, technical support and upgrade information

8.3 Costs

8.3.1 Forty percent (40%) of the total marks available are allocated to the contract cost. Costs must be submitted in Euro (ex VAT) for the following:

- Provision of software
- Cost per licensed user
- Support costs not included in the above, including training and hardware
- Any other costs, including recurring licence and maintenance/support costs.

8.3.2 The overall cost which will be evaluated will be calculated as follows:

- Cost must be submitted in the table provided in the response document
- Costs will then be marked on the basis of the following formula where 'n' represents the cost submitted by each candidate:

(Cost of the least expensive) X (maximum available marks)

Cost of 'n'

- Prices should be returned in the Response Document. All prices should be in Euro and exclusive of VAT. All prices quoted should hold firm for the duration of the contract. Quotes received must be inclusive of all costs, charges, taxes, customs, duties, transport and insurance charges (where appropriate) except VAT. All quotations and invoices must be in Euros.
- The prices quoted will remain fixed for acceptance for the period of 90 days from the date of submission of tender.

9. EVALUATION

Tenders that meet all of the qualification requirements will then be evaluated on the following Award Criteria.

- Suitability of proposed software
- Service Delivery Methodology and support
- Ultimate Cost

Submissions will be evaluated on a most economically advantageous basis. Marks will be awarded as shown in the tables below:



Criteria	Weighting	Maximum Marks Available	Minimum Score Required
Suitability of proposed software: Technical ability to fulfil all details as set out in the Specification of Requirements (as per Section 3 above)	70	350	210
Service delivery methodology and support (as per 8.2 above)	50	250	150
Ultimate Cost	N/A	400	N/A
Total		1000	

Tenders are required to achieve a minimum rating of “Good” (210 marks) for the ‘Suitability of proposed software’ criteria.

Tenderers should be aware that detailed weightings have been determined prior to the evaluation of ‘RFT’ submissions and that the table below reflects this. Marks awarded are at the discretion of FIOSRÚ and will not be subject to change.

Rating (per item)	Score	Basis
Excellent	5	Demonstrated excellent high-level expertise and understanding of the brief
Very Good	4	Demonstrated significant expertise high-level expertise and/or understanding of the brief
Good	3	Demonstrated good expertise and/or understanding of the brief
Fair	2	Limited expertise with limited detail supplied.
Poor	1	Very limited expertise or insufficient details supplied to allow a higher rating.
No evidence/ not rated	0	No expertise in the area or no information supplied.

10. FURTHER INFORMATION

- 10.1** The successful tenderer will be required to supply all materials, supplies and equipment relating to the contract.



- 10.2** The successful tenderer shall be responsible for the general behaviour, deportment, integrity and honesty of the staff employed and shall immediately remove from the building any employee if requested by the Ombudsman.
- 10.3** All costs incurred by tenderers in relation to their participation in this procurement competition shall be borne by and are matter for discharge by the tenderers exclusively.
- 10.4** Any conflict of interest or potential conflict of interest on the part of a tenderer, individual employees, agents, or subcontractors of a tenderer must be fully disclosed to the Contracting Authority as soon as the conflict or potential conflict is or becomes apparent.
- 10.5** The successful supplier will be expected to maintain tax clearance status throughout the duration of the Agreement. A valid tax clearance certificate (or equivalent) must be submitted annually to the Finance unit in the Fiosrú.
- 10.6** This Agreement may be concluded at any time on 30 days' notice in writing by either party without penalty with one exception where it may be concluded immediately if the security of the Fiosrú premises, personnel or systems is considered by Fiosrú to be compromised due to the actions / or inaction of the service provider.
- The successful service provider agrees that all information and data provided to it by the Commission for the purposes of the Agreement is confidential and that all reasonable measures will be taken to ensure, both during and after the terms of this Agreement, or after its termination, that no third party shall have access to said information or data, whether held electronically or otherwise, save with the prior written permission of the Commission.
- 10.7** The successful service provider and its workforce shall accept the provisions of the Official Secrets Act, Data Protection Act, and the Commission's Health and Safety Statement.
- 10.8** The successful service provider must confirm that they will comply with all legal obligations in relation to Health, Safety and Welfare at Work Acts. All tasks must be completed in a professional, safe and conscientious manner.
- 10.9** Payment will be processed in arrears on receipt of invoice for services rendered to a satisfactory standard. Payment terms are subject to the Prompt Payment of Accounts Act, 1997.



11. SUBMISSION

11.1 Closing Date

Tenders must be submitted via the post-box facility on www.etenders.gov.ie and must be received by Wednesday the 15th of October at 17:00. Submissions should be titled “Tender for the Provision of Forensic Software.

11.2 Enquiries

Queries and clarifications arising from this Tender should be submitted via eTenders by Friday the 3rd of October at 12:00. Any information resulting from queries will be available on eTenders.

11.3 Compliance

By Submitting a proposal in response to this RFT, the Tenderer agrees to all the statements, terms and conditions contained within this document.



Appendix A

FORM OF DIRECTIONS ON DATA PROTECTION AND SECURITY FOR EXISTING CONTRACTS UNDER FRAMEWORK AGREEMENTS

1. The Office for the Police Ombudsman (the “Contracting Authority”) and (COMPANY NAME) (“the Contractor”) entered into an Agreement for the provision Mobile Forensic Software in December 2025 (the “Agreement”) and a Confidentiality Agreement in December 2025 (the “Confidentiality Agreement”).
2. The Office for the Police Ombudsman (the “Client”) and the Contractor subsequently entered into a Services Contract pursuant to the Agreement in November (the “Agreement”).
3. Under clause 5.1 of the Confidentiality Agreement, the Contractor undertakes:
“to comply with all directions of the Contracting Authority and the Clients with regard to the use and application of all and any Confidential Information or data (including personal data as defined in the Data Protection Acts 1988 and 2003).”
4. Under Clause 7B of the Agreement, the Contractor undertakes:
“to comply with all reasonable directions of the Client with regard to the use and application of all and any of its Confidential Information”.
5. Further to the above provisions of the Confidentiality Agreement and the Agreement, the Client hereby directs the Contractor to comply with the following:
 - I. to comply with all applicable national and EU data protection laws, regulations and guidelines, including but not limited to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the “General Data Protection Regulation”), and any guidelines and codes of practice issued by the Office of the Data Protection Commissioner or other supervisory authority for data protection in Ireland (the “Data Protection Laws”);
 - II. to process the personal data described in Schedule A (the “Personal Data”) only on the written instructions of the Client;
 - III. to implement appropriate technical and organisational measures, to be reviewed and approved by the Client, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be



protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

- IV. to ensure that all personnel who have access to and/or process the Personal Data are obliged to keep the Personal Data confidential;
- V. not to transfer the Personal Data outside of the European Economic Area unless the prior written consent of the Client has been obtained and the following conditions are fulfilled;
 - a) appropriate safeguards are in place in relation to the transfer, to ensure that Personal Data is adequately protected in accordance with Chapter V of Regulation 2016/679 (General Data Protection Regulation);
 - b) the Data Subject (as defined under the Data Protection Laws) has enforceable rights and effective legal remedies;
 - c) the Contractor complies with its obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and
 - d) the Contractor complies with reasonable instructions notified to it in advance by the Client with respect to the processing of the Personal Data;
- VI. to promptly notify the Client if it receives a Data Subject access request (which means a request made by a Data Subject in accordance with rights granted under the Data Protection Laws to access his or her Personal Data;) to have access to any Personal Data or any other complaint, correspondence, notice, request any order of the Court or request of any regulatory or government body relating to the Client's obligations under the Data Protection Laws and to provide full co-operation and assistance to the Client in relation to any such complaint, order or request (including, without limitation, by allowing Data Subjects to have access to their data);
- VII. without undue delay to report in writing to the Client any data compromise involving Personal Data, or any circumstances that could have resulted in unauthorised access to or disclosure of Personal Data;
- VIII. to assist the Client in ensuring compliance with its obligations under the Data Protection Laws with respect to security, impact assessments and consultations with supervisory authorities and regulators;



- IX. at the written direction of the Client, to amend, delete or return Personal Data and copies thereof to the Client on termination of the Agreement unless the Contractor is required by the laws of any member of the European Union or by the laws of the European Union applicable to the Contractor to store the Personal Data;
- X. to permit the Client, the Office of the Data Protection Commissioner or other supervisory authority for data protection in Ireland and or their nominee to conduct audits and or inspections of the Contractor's facilities, and to have access to all data protection, confidentiality and security procedures, data equipment, mechanisms, documentation, databases, archives, data storage devices, electronic communications and storage systems used by the Contractor in any way for the provision of services under the Agreement and to comply with all reasonable directions of the Client arising out of any such inspection, audit or review;
- XI. to fully comply with, and implement policies which are communicated or notified to the Contractor by the Client from time to time;
- XII. to take all reasonable precautions to preserve the integrity of any Personal Data which it processes and to prevent any corruption or loss of such Personal Data;
- XIII. to ensure that a back-up copy of any and all Personal Data is made [insert frequency] and this copy is recorded on media from which the data can be reloaded if there is any corruption or loss of the data;
- XIV. in such an event and if attributable to any default by the Contractor or any Sub-contractor, to promptly restore the Personal Data at its own expense or, at the Client's option, reimburse the Client for any reasonable expenses it incurs in having the Personal Data restored by a third party;
- XV. to enter into a written agreement with third-party processor incorporating terms which are substantially similar to those set out in these Directions as between the Client and the Contractor;
- XVI. to maintain complete and accurate records and information to demonstrate its compliance with these Directions and to allow for inspections and contribute to any audits by the Client or the Client's designated auditor.

Processing, Personal Data and Data Subjects

1. Processing by the Contractor

- 1.1 Subject matter of processing:** all information, whether in oral or written (including electronic) form, created by or in any way originating with by the Contracting Authority



and/or any Framework Client (including but not limited to his/her employees, agents, independent contractors and/or Sub-contractors) and all information that is the output of any computer processing, or other electronic manipulation of any information that was created by or in any way originating with Contracting Authority and/or any Framework Client provided under the Agreement which relates to an identified or identifiable natural person;

1.2 Nature of processing [Providing Mobile Forensic Software to the Office for the Police Ombudsman]

1.3 Purpose of processing: to allow the Contractor to provide the services under the Agreement or the Contract.

1.4 Duration of the processing: The Term of the Contract.

2. Types of personal data [Names, Address, DOB, Sex, Contact Details, Health Data, Images, Third Party Details, Criminal History, Ethnicity, Religious Beliefs, Mental Health Status, Medical Data]

Categories of data subject [Fiosrú Staff, Members of the Public, An Garda Síochána Members]