Framework Agreement

on
National Contact Points
in the context of the
Smart Open Services for European Patients Project (epSOS)
(version 2)

Framework Agreement

on
National Contact Points
in the context of the
Smart Open Services for European Patients Project (epSOS)

Preamble

- The epSOS Large Scale Pilot Project has been established to develop and test a pilot system of cross-border data sharing to support patient care delivered to European citizens outside their usual state of residence by means of a shareable electronic Patient Summary and ePrescription.

- The Framework Agreement and its annexes is designed to establish the necessary level of trust to ensure that Health Professionals (Art 3 lit f Directive 2011/24/EU) can rely upon the integrity of the data that will support their decisions, that suitable systems of security exist to ensure that data cannot be accessed by unauthorized parties, and that patients' rights of informed consent to data sharing are duly respected by all parties.

- This Framework Agreement provides a blueprint for national level contractual agreements, where required[1], to create a National Contact Point [hereinafter NCP] as a legal entity entitled to process patient data in the context of the epSOS pilot.

- The Framework Agreement also sets out the core duties of the NCP and its partners so that the NCPs, once created, may contract on a common basis with their local partners (Healthcare Providers [Art 3 lit g Directive 2011/24/EU], Health Professionals and Points of Care) to deliver the epSOS services to Patients (Art 3 lit h Directive 2011/24/EU).

- Annexes I and II of the Framework Agreement give further guidance on the information to be given to Patients and Health Professionals on their rights and duties within epSOS.

- The articles of the Framework Agreement and its annexes shall be transposed into:

  o (where necessary) Contracts under applicable national law to establish epSOS NCPs and

  o (where necessary) Contracts under applicable national law to designate Points of Care from within existing Healthcare Providers as epSOS Points of Care.

- The terms of this Framework Agreement and its annexes may be modified during transposition into local contracts and guidelines only in so far as it is necessary to do so in order to comply with local law or custom.

- The contractual agreements established at national level to create the NCPs shall be certified as conformant to epSOS principals by the Project Steering Board.

---

[1] Some Participating Nations may not need to establish NCPs by contract if, for example, the national administration provides the service itself.

1. The epSOS pilot – Creation of the epSOS National Contact Point (NCP)

1.1. The epSOS pilot is an initiative of several European Participating Nations to develop and test a system for access to health data in cross-border situations to support patient care delivered to European citizens outside their usual state of residence by means of a common epSOS electronic patient summary and a common epSOS e-prescription.

1.2. The national and regional Departments of Health and their related eHealth Competence Centres are beneficiaries of Grant Agreement number 224991 of the European Commission and its associated Consortium Agreement.

1.3. In accordance with the Grant Agreement the beneficiaries have contracted with the European Commission and each other to ensure that a number of healthcare establishments within their territory will provide one or more test sites for the epSOS Pilot – hereinafter known as a healthcare provider.

1.4. Each participating nation shall appoint one legal entity to act as NCP. Where this function is federated across several organisations one entity shall act on behalf of the others to be the liaison point for NCPs from other epSOS nations.

1.5. In the case of regional beneficiaries one NCP will represent all regional beneficiaries.

1.6. The NCP in each PN shall be created under local law on the basis of the present framework agreement.

2. Core Characteristics of the epSOS National Contact Point (NCP) (Terms to be included in all national contracts relating to epSOS)

2.1. The NCP shall be a legal entity which is legally competent to contract with other organisations in order to collaboratively carry out its duties and responsibilities in epSOS.

2.2. The NCP shall contract with epSOS Healthcare Providers to provide epSOS services to Patients.

2.3. The semantic transformation is performed according to the translation, mapping and trans-coding carried out by designated competent legal entities in the epSOS countries

    2.3.1. the responsibility for the *accuracy* and integrity of the process is with each national designated competent legal entity for such semantic processing

    2.3.2. liability for errors in the semantic mapping is shared between the parties who have been involved in the production of the PS or ePrescription.

    2.3.3. Pilot sites are not liable for any patient safety adverse events attributed to semantic mapping, save for any contributory negligence in interpreting the data.

2.4. The epSOS NCP shall provide a gateway service, a request port and a semantic mapping service in order to enable it to execute the core steps in the epSOS use cases (see end note).

2.5. The NCP together with its national contractual partners shall collectively fulfil all technical and organisational requirements for secure and confidential transfer or

storage of data necessary to perform the steps outlined above. Specifically the NCP shall:

> 2.5.1. be technically competent to provide a gateway for epSOS information transfer;
>
> 2.5.2. be legally recognised as a data controller or data processor in accordance with domestic data protection legislation;
>
> 2.5.3. be legally competent to execute contractual agreements with all domestic partners in compliance with domestic data protection legislation;
>
> 2.5.4. be legally competent to enforce audit and corrective action emerging from audits;
>
> 2.5.5. be technically competent to validate the identity of Patients and patient consent of its territory (acting as country A);
>
> 2.5.6. maintain the local versions of the epSOS semantic value sets.

3. General Duties and responsibilities of the epSOS NCP (terms to be embodied in the national contracts creating the NCPs)

3.1. The epSOS NCP shall establish appropriate security and data protection systems to conform to epSOS requirements as well as all applicable national requirements.

3.2. The epSOS NCP shall take all reasonable steps to ensure data security (including data confidentiality, integrity, authenticity, availability and non-repudiation).

The epSOS NCP shall establish an appropriate system to validate the identity and accreditation of Health Professionals and Healthcare Providers on its territory who may legally receive data originating from an epSOS NCP in another nation. The epSOS NCP shall establish an appropriate system of audit trail so that records of data collected, processed, translated and transmitted may be duly inspected by official bodies if necessary as well as collected by NCP A from all parties concerned and handed over to a Patient or a Healthcare Provider requiring such information. The epSOS NCP shall assume responsibility for appropriate data collection on the execution of the pilot through the Points of Care on its territory and shall assume responsibility for the reporting of such data to the epSOS Project Partner(s) on its territory.

3.3. The epSOS NCP must ensure that nominative epSOS data is not transmitted to parties outside the NCP and its pilot partners.

3.4. The epSOS NCP shall maintain a helpdesk service to support the Health Professionals and Healthcare Providers in its territory.

3.5. The epSOS NCP maintain the communication on epSOS pilots at national level and links to the epSOS website.

4. epSOS NCP duties and responsibilities to other epSOS NCPs

4.1. The epSOS NCP shall be accountable to other epSOS NCPs for ensuring the security (confidentiality, integrity, availability, non repudiation and authenticity and auditability) of data processed on their territory.

4.2. The epSOS NCP shall be accountable to other epSOS NCPs for guaranteeing that all epSOS jointly agreed service specifications and requirements (legal, organisational, semantic and technical) are fulfilled.

4.3. **T**he epSOS NCP shall be accountable to other epSOS NCPs, represented through the PSB, for ensuring, conformance of all epSOS national pilot partners to jointly agreed service specifications and requirements.

4.4. The epSOS NCPs shall collaborate actively to the harmonisation of guidelines and appropriate practices to facilitate the establishment of the epSOS trusted domain.

4.5. The epSOS NCPs shall adopt the epSOS Information Governance framework that will comprise commonly adopted policies, processes and audit mechanisms.

4.6. The epSOS NCPs must ensure that national agreements with pilot partners include provisions for applying and regularly auditing the epSOS Information Governance framework. Such audit practices applied by NCPs shall be audited by an external independent auditor.

5. **Duties and responsibilities concerning epSOS Patient Consent (terms to be embodied in the national contracts creating the NCPs and contracts between NCPs and their partners as appropriate)**

5.1. No epSOS data shall be collected either directly from the Patient or indirectly from Healthcare Providers without the freely given, specific and informed consent of the Patient, according to national law of the country where treatment is provided.

5.2. The epSOS pilot shall be conducted on the basis of an opt-in system of consent; accordingly implied consent to epSOS data collection and processing shall not be permitted.

5.3. The epSOS NCP shall ensure (directly or through appropriate contractual agreements with their Points of Care that consent is obtained and documented for the creation of epSOS records (Patient Summary and ePrescription) if required by national law.

5.4. The epSOS NCP can establish a system which allows a patient to give a prior general agreement to access to his or her record by a Health Professional or Point of Care or Healthcare Provider abroad. The epSOS NCP shall establish with its partners a process which allows such general prior agreement, if required by national law of country A, to be validated at the Point of Care. Such validation procedures shall be e.g. by ticking a box to confirm patients' consent for access to their Patient Summary or ePrescriptions held in their home country and shall not be disruptive of the clinical workflows.

5.5. The epSOS NCP shall establish a system to allow a Point of Care providing services to an epSOS patient to document the validations of consent for release of data from the NCP to the Point of Care.

5.6. The epSOS NCP may establish a system for directly obtaining agreement from the patient in situations where prior generalised agreement has not been provided in country A, in all cases where country A permits such delegation of responsibility.

5.7. The epSOS NCP shall establish a consent override procedure to provide for exceptional cases where it is not possible to obtain consent or validation of consent because of the patient's incapacity including consent for minors. The epSOS NCP shall ensure that all the parties concerned with the pilot are able to comply with the requirements of patient consent to epSOS data collection and processing.

6. Duties and Responsibilities of the epSOS Pilot Partners under the epSOS Security Policy

6.1. The epSOS security policy creates a general security and data protection framework adapted to the epSOS information system needs.

6.2. The epSOS security policy address all elements of data flows in the pilot including national and cross-border data flows

6.3. The epSOS actors (epSOS NCPs, Health Professionals, Points of Care and Healthcare Providers) shall ensure that they are fully compliant with the Security Policy as set out in detail in Annex III.

7. Relationship between NCP and Points of Care, Health Professionals and Healthcare Providers

7.1. A number of partners in the epSOS pilots shall be legally established and recognised. They shall include Points of Care and Health Professionals, and may also include Healthcare Providers representing several Points of Care**.**

7.2. Each PN will identify a number of Healthcare Providers which will take part in the pilot. These shall include primary care providers (general practitioners and primary care clinics); secondary care providers (hospitals specialist secondary care providers); pharmacies (both public and private).

7.3. The Healthcare Provider shall sign a contract under local law with the NCP to which it is responsible.

7.4. The Healthcare Provider/NCP contract shall set out all the minimum requirements of the Point of Care and shall establish the legal relationship between them.

7.5. The Healthcare Provider/NCP contract shall set out minimum requirements for epSOS training for all health professionals who shall be active within the pilot.

7.6. The Healthcare Provider/NCP contract shall detail the duties of both parties with respect to maintaining the security of the epSOS pilot and all data flows.

7.7. The Healthcare Provider/NCP contract shall detail the duties of both parties with respect to ensuring that patient consent to collecting and processing epSOS data has been duly obtained and documented according to epSOS procedures.

8. Dispute resolution and applicable law

8.1. The co-operation between NCPs shall be ensured through the Grant Agreement.

8.2. Any conflicts arising between NCPs shall, in the first instance, be referred to the PSB. A request for arbitration may be filed with the European Court of Arbitration in the event of any dispute which cannot be resolved at project level.

9. Amendments of the Framework Agreement

9.1. Amendments to this Framework Agreement, its Annexes and any related epSOS policies which have been duly adopted in accordance with project procedure through the epSOS Project Steering Board (PSB), shall be translated and applied to the contracts for epSOS services as provided for in the preamble. The National

Authority Beneficiary (NAB) shall give appropriate publicity to the adopted amendments as well as the decision of the PSB not later than 4 weeks after the amendments have been adopted by the PSB.

9.2. Save from the NABs, all parties to the above mentioned contracts shall have the right to rescind the contract during the 16 weeks following the PSB decision.

9.3. Unless otherwise defined by the PSB, the amendments to the above mentioned contracts shall come into effect 16 weeks after the amendments have been adopted by the PSB.

ENDNOTE – Steps in epSOS Process

1. Health Professional in country B at a Point of Care accepts patient ID which may identify the patient as being eligible to take part in epSOS trial.

2. Health Professional in country B at a Point of Care confirms patient consent to access data in Country A; or Health Professional ticks the override box in cases where consent cannot be obtained because of patient incapacity. A Health Professional's query can be processed only with consent or override duly confirmed.

3. Health Professional in country B sends query to NCP in country B.

4. NCP in country B authenticates the Health Professional and Point of Care.

5. The NCP in country B queries NCP in country A for the requested patient data.

6. NCP in country A authenticates NCP in country B.

7. NCP in country A validates patient ID and local prior agreement (if applicable).

8. NCP in country A transmits the requested data to NCP in country B.

9. NCP in country B authenticates NCP in country A.

10. NCP in country B provides the requested data to Health Professional requestor.

ANNEX I. epSOS PRIVACY INFORMATION NOTICE

1. What is epSOS ?

epSOS – Smart Open Services for European Patients – is a large scale pilot project being conducted across several European countries to help European citizens access health services when they are outside their usual country of residence.

[Country/Region] is taking part in epSOS so you, as a citizen of [Country/Region], are entitled to make use of the epSOS services if you need medical care while in another participating country.

2. What are epSOS services

The aim of the epSOS Large Scale Pilot is to demonstrate that it is feasible for citizens of a European country to enjoy the benefits of electronic health services that they receive at home, when they travel abroad without compromising their rights to privacy and confidentiality. The two epSOS services that are offered on a pilot basis have been tested and appropriate safeguards required by European and national law have been taken.

Additionally, [name of NCP-A] guarantees that the level of security and protection of citizens rights to privacy have been ascertained to a level that has been considered appropriate by all countries and regions participating in this pilot. *Please consult the epSOS website www.epSOS.eu for a current list of piloting nations and regions.*

Each of these countries and regions, through a designated organisation, have undertaken to ensure that the participating Healthcare Providers and Health Professionals on their territory taking part in the epSOS pilot have adequate information and training about the pilot and the duties and responsibilities which must be assumed when offering these epSOS services. Please refer to the epSOS website for details on the epSOS pilot and the participation of [country name] in it.

3. Your data , Your Consent

The epSOS services will become available to you in participating countries and institutions only if you consent to provide access to your personal Patient Summaries/e-prescriptions to health professionals in the context of providing care to you while you are abroad. Please refer to the epSOS Terms and Conditions document for details on these services and the terms and conditions for their delivery.

[Here please insert a paragraph about

- consent to create a PS if needed by your country

- consent to **opt-in** the epSOS pilot so that your personal Patient Summaries/e-prescriptions can be made accessible for health professionals in participating countries and institutions, and how an opt-in consent can be given if needed by your country

- any exceptions to providing access in case of emergency (e.g. if prior consent has not been provided)]

When abroad in an actual care situation, the treating physician will need your consent to access your Patient Summaries/ePrescriptions.

If you have not provided your agreement to participate in the epSOS pilot in [country name] it is still possible to provide consent for access to data from the country you are visiting after reading and agreeing to (through signing) the epSOS Terms and Conditions and confirming your consent to the treating physician by confirming the following statement in a country where you require medical care:

 'I agree that my [name of electronic document as known in the MS] may be transferred to a registered Health Professional in [COUNRTY OF TREATMENT] for the purposes of providing me with medical care and/or medication.

ANNEX II. epSOS TERMS AND CONDITIONS[2]

The epSOS services are offered in conformance to epSOS safeguards and procedures, established collectively and with active representation from participating Points of Care. Specifically:

1. **Terms and Conditions relating to the Patient Summary and ePrescription**

    1.1. The purpose of access to information contained in a Patient Summary is to enable Health Professionals in countries other than the Patient's country of residence to make an informed decision and to improve patient care. The project will also enable Patients to have ePrescriptions from their country of residence dispensed at designated epSOS pharmacies in other participating countries. The use of the epSOS services is voluntary on the part of the Patient. The epSOS Patient Summary (PS) does not hold detailed medical history or details of clinical conditions or the full set of the prescriptions and dispensations.

    1.2. The Patient Summary contains a common and agreed structure for all the European countries and reliable information of where the patient is insured. The Patient Summary is divided into three main sections: Patient Administrative Data, Patient Clinical Data and Information about the Patient Summary itself.

    1.3. Each country is responsible for the content of the Patient Summary and its creation. Information about how the Patient Summary is generated (ie by direct human intervention of a Health Professional; automatically generated using the national data bases; a mixed approach, validated by the human intervention) is included in the third section of PS.

    1.4. When a medical record is created in another country such information is not included into the PS. It will be included into the patients' records in the usual country of residence only if such records are sent back to the Patients' country of residence. Such correspondence is not part of epSOS and happens only in accordance with usual practice at the foreign point of care. Only the fields [National healthcare patient ID], [Given name], [Family name/Surname], [Date of Birth] will be always present in the PS. The rest of the fields are populated according to what data is held in the patient's country of residence where the Patient Summary is generated.

    1.5. It is important to note that, if a Patient has decided to hide information in his country, this hidden information will not appear in the epSOS dataset neither will there be any kind of flag in the PS to alert this fact.

    1.6. Use of the epSOS services does not alter obligations to fulfill legal requirements existing in the country where medical care is provided to the Patients participating in the epSOS pilot.

    1.7. Health data will be recorded and stored in medical records at the point of care according to the regulations applicable in the treating country. epSOS services do not involve any transfer of such medical data to the Patient's country of usual residence.

---

[2] Piloting Nations must also inform the patient if the use of epSOS services will be at a cost for the patient. If no cost will occur for the patient, this information is not necessary.

2. Terms and Conditions relating to the Privacy

2.1. Access to data is permitted provided that patient consent has been granted in accordance with national law, and the purpose of access is to provide medical care for the Patient. If the Patient decides not to give his/her consent, this can be recorded in the country where the Patient Summary is created. The Patient can also decline the use of epSOS services at the Point of Care, whereas no access is allowed.

2.2. If consent has not been provided already at the country of affiliation or where the Patient is insured, it is still possible to obtain it at a Point of Care in foreign country. In this event such consent must be freely given, must be specific to the care encounter and the Patient must be informed about which data are to be collected and to what purpose they will be put.

> 2.2.1. Consent must always be confirmed at the Point of Care, provided that the Patient is not a minor or has diminished capacities[3]. Patients will be duly informed and provided with the respective information as needed in their own language at the Point of Care.

> 2.2.2. Patient consent is recorded and logged electronically before data request is submitted.

> 2.2.3. Access to information may also be granted by the relevant authority in the country of usual residence in emergency situations[4] when the patient´s life is at risk or it can be assumed that the Patient may suffer a very serious health risk if information is not given. The Patient will receive information of any such access that has taken places as soon as the Patient is able to receive such information.

2.3. The European Data Protection Directive (DPD), implemented in national law, gives the Patient right to obtain from the Data Controller:

"(a) without constraint, at reasonable intervals and without excessive delay or expense:

- *confirmation as to whether or not data relating to him[/her] are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,*

- *communication to him[/her] in an intelligible form [about] the data undergoing processing and of any available information as to their source,*

- *[communication to him/her of the concept] involved in any automatic processing of data concerning him[/her] at least in the case of the automated decisions referred to in Article 15 (1) [of the DPD];*

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;"

2.4. Provisions have been made that any person who has suffered damage as a result of an unlawful processing operation or of any data processing act incompatible with

---

[3] These cases are excluded from this phase of epSOS pilot services

4 i.e. the cases when data is necessary to avert *life-threatening situation* to someone's health, when the data subject is not able to give consent due e.g. to acute disease or accident. In such cases, the necessity from a medical point of view to collect/handle data, compensates for the requirement of a valid consent, regardless of given or not given prior or concrete consent

the national provisions adopted according to his/her national legislation is entitled to receive compensation from the controller for the damage suffered.

2.5. Any further questions can be addressed to: (Country contact details of national coordinator and Data Controller).

ANNEX III. epSOS SECURITY POLICY (epSOS SP)

1. The epSOS Security Policy

1.1. **Need and Scope**

Security is a critically important issue for epSOS. Without adequate security in place none of the epSOS services can be used in real-life environments. The epSOS Security Policy (epSOS SP) aims to create a secure operational environment for the service deployment which will be sufficient for protecting the epSOS data and processes, implementable and agreed by all participants. The epSOS Security Policy provides a secure operational environment for epSOS, helps develop a 'chain of trust' among epSOS actors and has been developed according to the provisions of the Technical Annex of the project and the contract. The Security Policy also specifies the obligations of service providers and users and must be implemented and periodically audited by all epSOS partners, as described below.

1.2. **Principle and Objectives**

1.2.1.   Principle

All epSOS data and processes must be adequately protected. The network built among the epSOS partners should also not add any unacceptable new risk within any partner organization. Appropriate technologies and procedures must be used to ensure that data is stored processed and transmitted securely over the network built among the epSOS partners and is only disclosed to authorized parties.

Information security is generally characterized as the protection of:

a. Confidentiality (information is protected from unauthorized access or unintended disclosure – only authorized users have access to the information and other system resources),

b. Integrity (information is protected from unauthorized modification) and

c. Availability (resources are available, without unreasonable delay - authorized users are able to access information and the related means when they need it).

The epSOS Security Policy should help to ensure and enforce the above. It should also provide means of proof and essential checks, which establish users' trust in the given information.

1.2.2.   Objectives

The objective of the epSOS Security Policy is to establish the basic security provisions that must be satisfied in order to ensure the security of data and system continuity and to prevent and minimise the impact of security incidents by implementing a stable, reliable and secure infrastructure.

More specifically, the epSOS Security Policy objectives are:

a. To make epSOS actors sensitive in the operated means of protection and in the risks which they cover.

b. To create a general security framework adapted to the epSOS information system needs, which should be observed by those in charge of epSOS processes; it should be implemented by putting in place measures and

procedures in order to ensure the epSOS information and epSOS information system and infrastructure security.

c. To promote cooperation between various epSOS actors in order to jointly elaborate and put in place those measures, instructions and procedures.

d. To enhance user and Patient' trust in the information system.

e. To ensure that the information system in place respects the National and European legislation on privacy and data protection in force.

The epSOS security policy is constructed under the principle of well-proportioned answer to the incurred risk.

1.3. **Security Rules**

The following general security rules are required and apply for the epSOS data exchange model:

SR 1	epSOS data flows must be adequately protected, as specified in the ISO 27000 series international standards or equivalent.
SR 2	End users must be unambiguously identified by national infrastructure before being provided access to the system.
SR 3	Mutual authentication between End Users and the national infrastructures' identity providers is needed when connecting to the system.
SR 4	End user identification and authentication procedures in place must be audited according to the epSOS security audit policy.
SR 5	The epSOS security audit policy must be implemented. Audit policy is defined by the epSOS PSB
SR 6	Mutual Authentication between national contact point providers (NCPs) of different Member State is needed when initiating a trans European (cross border) information flow.
SR 7	Non-repudiation procedures must be implemented between the User-Originator and the User-Receiver of documents and messages
SR 8	All epSOS actors in a Country B must ensure that any medical document is forwarded only to the user that has been authorized to access the document.
SR 9	The software used to implement the NCP gateway must conform to the technical specifications of epSOS architecture and common components (D3.3.2, D3.4.2 and D3.9.1)

Rules SR2, SR3 and SR4 are national (national level) competency, while rules SR5, SR6, SR7, and SR8 are a pan European (epSOS level) competency.

In addition, epSOS actors and processes must also take into account the relevant security provisions of the security recommendations of the Commission Recommendation on cross-border interoperability of electronic health record systems (Rec. 2008/594/EC).

1.4. **Security Audit**

A security audit must be conducted yearly to audit the systems by ISO/IEC 17799 or ISO/IEC 27001, or equivalent level standards, according to the above listed requirements and the guidelines provided in D3.8.2. in this respect. Audit will be based on the epSOS Security Audit policy, described in Chapter 2 of this Security Policy.

1.5. **Document update policy**

A Security Expert Group (SEG) set up and operating within the TPM function of epSOS, will continually follow-up and propose revisions of the security policy to WP2.2. Proposed amendments will be placed on the PSB agenda twice a year or as otherwise deemed necessary.

Clear and justified proposals for Security Policy review arising from the implementation activities need to be accompanied by an assessment of their impact on the rest of the work packages.

1.6. **References**

[D3.7 MD] "WP3.7_D3.7.2_ Security Service_V04.pdf", REGLOM, epSOS 2010

[epSOS Annex I] epSOS Annex I – "Description of Work", EMP/S.O.S. LSP-eHealth team, 2008-06-30

[FWA] D2.1 Legal and regulatory constraints on epSOS, WP2.1, epSOS, 2009-01-31

1.7. **Further Requirements and Recommendations**

All epSOS actors must respect the provisions of this Security Policy.

The epSOS NCPs shall collaborate actively to the harmonisation of guidelines and appropriate practices for the epSOS Security Policy and its implementation[5].

2. **The epSOS Security Audit Policy**

2.1. **Objectives**

In compliance with the provisions of the epSOS Security Policy (SP), the epSOS Security Audit shall observe the following general requirements:

- It shall cover both the epSOS Security Policy and the ISO 27000/2 standard requirements.

---

[5] According to FWA clause 4.4.

- The epSOS Security Audit shall focus on confidentiality and integrity needs more so than availability needs.
- The epSOS Security Audit shall include an assessment of compliance to national legislation.
- The epSOS Security Audit Procedure is conducted by national auditors, using ISO based procedures.
- Each national epSOS NCP must pass successfully annual security audits.
- Successful completion of the Initial Audit shall certify that data and privacy protection procedures are in place as a pre-requisite to entering the Operation Phase of the Pilot.
- Besides the NCP infrastructure also the epSOS Central Services need to be audited.

2.2. Basic Provisions for the Audit Procedure

The epSOS security audit procedure is based on the following provisions:

- An internal audit process will be followed, where the National Authority Beneficiary (NAB) selects its own auditor. The audit should be performed by an auditor that is certified to international standards and accredited by national law. The ISO 27002 standard shall provide the framework for epSOS audit.
- In case of a serious non-conformity or dispute an escalation process will be carried out by the PSB, which may include the delegation of an epSOS independent certified auditor to perform an independent audit in the MS in question.
- The PSB will appoint a group of security experts in the legal and technical domain, that will coordinate and review the Member States implementation of the Security Policy.
- This process will be mainly desktop review of audit reports provided in a standardized epSOS Audit Report format and may include onsite visits which will in addition be part of learning and exchange of good practices in epSOS.