Secure management of IoT devices lifecycle through identities, trust and distributed ledgers

D8.4: NEC - Requirement No. 5

Document Summary Information

Grant Agreement No	101020416	**Acronym**	ERATOSTHENES
Full Title	Secure management of IoT devices lifecycle through identities, trust and distributed ledgers		
Start Date	01/10/2021	**Duration**	42 months
Project URL	www.eratosthenes-project.eu		
Deliverable	NEC - Requirement No. 5		
Work Package	WP8		
Contractual due date	30/07/2022	**Actual submission date**	28/07/2022
Nature	Ethics	**Dissemination Level**	Public
Responsible author	DBC	**Lead Beneficiary**	DBC
Authors	George Athanasiou, Sara Nabaraoui (DBC)		
Internal reviewers	Hui Song (DBC)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101020416.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V1	20/06/2022	40%	Initial Deliverable Structure & Basic Processes.	George Athanasiou, Sara Nabaraoui (DBC)
V2	15/07/2022	70%	Assessment is completed.	George Athanasiou, Sara Nabaraoui (DBC)
V3	22/07/2022	100%	Final version	George Athanasiou, Sara Nabaraoui (DBC)
V4	28/07/2022	100%	Final version after quality review	Hui Song (DBC)

Disclaimer

Copyright message

Table of Contents

1 Executive summary

ERATOSTHENES NEC - Requirement No. 5 document responds to the forth "ethics requirement" by the European Commission by analysing materials which will be imported to/exported from the EU within the project. This is regarded as work performed in WP8 (Ethics Requirements) and this report is the forth deliverable on requirement No 5. This deliverable complements the reports D8.1, D8.2, and D8.3.

2 Introduction

2.1 Mapping ERATOSTHENES outputs

The purpose of this section is to map ERATOSTHENES Grant Agreement (GA) commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to ERATOSTHENES GA Deliverable & Tasks Descriptions

ERATOSTHENES GA Component Title	ERATOSTHENES GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D8.4 NEC - Requirement No. 5	D8.4 will include: • Details on the materials which will be imported to/exported from the EU. • In case activities undertaken in non-EU countries involves material import/export, copies of import/ export authorisations, as required by national/EU legislation must be obtained and kept on file.	*1-7*	*The current report responds to the forth 'ethics requirement' received from the European Commission.*
WP/TASKS			
WP8	This work package sets out the 'ethics requirements' that the project must comply with.	*1-7*	*Chapters 1-7 include: - Details on the materials which will be imported to/exported from the EU. - In case activities undertaken in non-EU countries involves material import/export, copies of import/ export authorisations, as required by national/EU legislation must be obtained and kept on file.*

2.2 Deliverable overview and report structure

The present report is structured around 7 Chapters as follows:

- Chapter 1: Executive summary of the deliverable.
- Chapter 2: Introduction and general overview of the requirements of the deliverable in comparison to what is mentioned in the Grant Agreement.
- Chapter 3: Transfer of personal data to third countries or international organisations and GDPR.
- Chapter 4: Identification of non-EU beneficiaries involved in ERATOSTHENES.
- Chapter 5: Relevant national laws on transfer of personal data.
- Chapter 6: Analysis of data processing activities in ERATOSTHENES involving non-EU countries.
- Chapter 7: Conclusions.

3 Transfer of personal data to third countries or international organisations and GDPR

GDPR[1] dictates the conditions under which personal data may be transferred to third countries or international organisations. Whenever personal data which are undergoing processing or are intended for processing are transferred to a third country or to an international organisation, Chapter V of the GDPR applies.

Basically, Chapter V of the GDPR ensures that the protection that the GDPR offers to a natural person regarding its personal data travels with the data when it leaves the EEA territory. That is why the GDPR restricts the transfer of personal data outside the EEA. Only when one of the 'transfer mechanisms' listed in articles 45 to 47 of the GDPR is complied with, the transfer of personal data to a third country or international organisation may take place.

According to article 45 (1) of the GDPR, a transfer of personal data to a third country or an international organisation may take place where the European Commission (EC) has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection, i.e. if the EC has made an adequacy finding for the country or territory concerned. In that case, the transfer of personal data to that third country or international organisation will not require any specific authorisation.

In the absence of such an adequacy decision, according to article 46 (1) of the GDPR, personal data may be transferred to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.

These appropriate safeguards may be provided for by:

- A legally binding and enforceable instrument between public authorities or bodies

  This Is not an appropriate safeguard when the data exporter (based in the EU) or the data Importer (based outside the EU) is a private body or an individual.

- Binding corporate rules (BCR's)

  These are personal data protection policies that serve as internal rules for data transfers within multinational companies. BCR's have to be authorised by the supervisory authority(ies) before any transfer can be performed.

- Standard data protection clauses (adopted by the Commission or adopted by a supervisory authority and approved by the Commission)

  These are 'model contract clauses' that should in their entirety be incorporated into a contract between the data exporter (based in the EU) and the data importer (based outside the EU), before the transfer can be performed. The clauses contain contractual obligations on the data exporter and the data importer as well as rights for the individuals whose personal data is transferred.

- An approved code of conduct (together with commitments of the data importer in the third country to apply the appropriate safeguards)

  This option is newly introduced by the GDPR and no approved codes of conduct are yet in use.

[1] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_el

- An approved certification mechanism (together with commitments of the data importer in the third country to apply the appropriate safeguards)

  This option is newly introduced by the GDPR and no approved codes of conduct are yet in use.

- Contractual clauses between the data exporter and the data importer in the third country or international organisation, authorised by the competent supervisory authority.

  These are data protection clauses incorporated in a contract between the data exporter and the data importer that haven been individually authorised by the supervisory authority of the country from which the data are exported.

- Administrative arrangements between public authorities or bodies which include enforceable and effective rights for the individuals whose personal data is transferred, and which have been authorised by a supervisory authority.

If, however no adequacy decision or appropriate safeguards as mentioned above are in place, a transfer of personal data to a third country or an international organisation can only take place if one of the **derogations for specific situations** listed in **article 49 of the GDPR**[2] applies.

This is the case when:

- the data subject has explicitly *consented* to the proposed transfer, after having been informed of the possible risks thereof in absence of adequacy decision or appropriate safeguards;

- the transfer is *necessary for the performance of a contract between the data subject and the controller* or the implementation of pre-contractual measures taken at the data subject's request;

- the transfer is *necessary for the conclusion or performance of a contract concluded in the interest of the data subject* between the controller and another natural or legal person;

- the transfer is *necessary for important reasons of public interest;*

- the transfer is *necessary for the establishment, exercise or defense of legal claims;*

- the transfer is *necessary in order to protect the vital interests of the data subject or of other persons,* where the data subject is physically or legally *incapable of giving consent;*

- the transfer is made from a *register* which according to Union or Member State law is *intended to provide information to the public and which is open to consultation* either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

If the transfer cannot be based on one of the derogations set out above, a transfer may only take place if it is non-repetitive, concerns only a number of data subjects, is necessary for the purposes of compelling legitimate interests of the controller that are not overridden by the data subject and the controller has provided suitable safeguards with regard to the protection of personal data.

[2] https://gdpr-info.eu/art-49-gdpr/

Besides the requirements resulting from Chapter V of the GDPR, it should not be forgotten that other requirements laid down in the GDPR may also apply, given that *a transfer of personal data to a non-EU country or international organisation in itself implies a processing activity*.

As presented before, every processing of personal data should be supported by one of the 6 legal bases listed in the GDPR. Given that a transfer of personal data to a third country or international organisation implies a processing activity, it should not only be justified by one of the transfer mechanisms discussed, but it should also be backed by a legal basis.

Pursuant to **article 6 of the GDPR[3],** any processing of personal data can only be lawful if and to the extent that one of the following **legal bases** apply:

- The data subject has given *consent* to the processing of his/her personal data for one or more specific purposes;
- The processing is *necessary for the performance of a contract* to which the data subject is party or the processing is necessary in order to take steps at the request of the data subject prior to entering into a contract;
- The processing is *necessary for compliance with a legal obligation* to which the controller is subject;
- The processing is *necessary in order to protect the vital interests* of the data subject or of another natural person;
- The processing is *necessary for the performance of a task carried out in the public interest* or in the exercise of official authority vested in the controller;
- The processing is *necessary for the purposes of the legitimate interests* pursued by the controller or by a third party.

This legal basis does not apply however when these interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Thus, when a transfer of personal data to a third country or international organisation is envisaged, the controller or processor must not only comply with the specific requirements of Chapter V of the GDPR, but must also be able the show which legal basis in the list of article 6 of the GDPR applies in order for the transfer to be lawful.

[3] https://gdpr-info.eu/art-6-gdpr/

4 Identification of non-EU beneficiaries involved in ERATOSTHENES

The following non-EU beneficiaries are part of ERATOSTHENES project:

IDIADA Automotive Technology UK Ltd

IDIADA Automotive Technology UK Ltd is a wholly owned subsidiary of IDIADA Automotive Technology SA and therefore part of the Applus+ group of companies. IDIADA UK has three offices with the centre of excellence for vehicle connectivity and autonomy based at the Cambridge office. This office has 30 years' experience in the design and development of automotive electronics and software.

Link to the partner: Subsidiary 100% of IDIADA AUTOMOTIVE TECHNOLOGY SA

Tasks: The role of IDIADA UK in the project is to provide the equipment and expertise for the IDAPT OBU (On-board Unit) in a vehicle and IDAPT in a RSU (Road Side Unit) role. IDIADA UK's main efforts is in supporting the development of the connected vehicle pilot demonstrator and scenarios expected in WP5 (T5.3.) and the system integration activity (T5.1). This also includes supporting the integration of the PUF with the IDAPT unit. IDIADA UK will also support tasks in WP1 (T1.2/T1.4), WP3 (T3.1 / T3.2), WP4 (T4.4) and dissemination activities in WP6 (T6.1/T6.6).

TELLU IoT AS

TELLU provides eHealth services spanning from welfare services for keeping elderly safe at home to remote supervision of patients with chronical diseases such as COPD, diabetes, and kidney, as well as more acute diseases such as Covid-19 patients. Tellu is market leader in welfare technologies in Norway. Tellu is a technology company and develops and delivers an IoT based eHealth platform named TelluCloud (provided as a PaaS) for connectivity, device management, edge computing, data gathering, data processing and presentation, and complete SaaS solutions for remote supervision, patient alarm systems, personnel safety, Next of kin apps etc. Tellu also delivers response centre services at a national level as well as integration with other response centre solutions. TelluCloud includes a Personal Health gateway (PHG) to cope with complete management and trustworthy execution and processing of health data across the IoT, edge and cloud space. Tellu also owns and host an Open Source edge computing framework, ThingML, that copes with specific complexities of IoT and edge computing, raising the level of abstraction to cope with the large heterogeneity in the IoT and edge space (https://github.com/TelluIoT/ThingML). Tellu both provides its platform as part of a system of systems with service providers and partners to deliver business critical services and they deliver stand-alone SaaS to end customers.

Tasks: TELLU is an end-user in ERATOSTHENES and as such has a primal role in the end-user requirements and pilot scenarios definition and structuring in WP1, task 1.2. TELLU also leads the pilot 2 implementation and validation activities in task 5.4 – healthcare. TELLU also supports SINTEF in task 2.3 on the Automated Deployment of Trust Agents and support horizontal activities in dissemination, communication (WP6) and management reporting tasks (WP7).

SINTEF SA

SINTEF is the fourth largest independent research organisation in Europe, with 2100 employees of which about 46% of the researchers hold a doctorate degree. Every year, it supports 2000 Norwegian and overseas companies via research and development activities. SINTEF Digital is one of 8 research divisions within the SINTEF Group, with

300 employees, and provides research-based expertise, services and products including micro-technology, communication and software technology, computational software, information systems, security and safety.

The research group on Secure IoT Software, which participates in the project, is part of the Software and Service Innovation department within the Digital division. This group is in Oslo, Norway, and focuses on research in software engineering and security, with particular interest in supporting DevOps in the domains of Internet of Things, cloud computing, cybersecurity, and the risk management in software development.

Tasks: SINTEF is the ERATOSTHENES quality manager and responsible for the data management and risks management tasks (WP7). Having particular expertise in lifecycle management in the area of IoT and trust in related environments is leading task 2.3 (Automated Deployment of Trust Agents) and task 2.5 (Automated recovery process of trust manager) in WP2. Additionally, SINTEF strongly contributes to WP1 activities in the methodological trust framework and identity management architecture. Further, SINTEG contributes to the task of system integration (WP5, task 5.1) as well as in the ERATOSTHENES horizontal tasks, dissemination and communication activities.

5 Relevant national laws on transfer of personal data

5.1 Norway (NO)

Although Norway is not part of the European Union, Norway is a member of the European Economic Area (EEA) 6, making it part of the EU's single market. That is why, by decision of 6 July 2018, the EEA Joint Committee announced the incorporation of the General Data Protection Regulation (GDPR) into the EEA Agreement, making the GDPR directly applicable to the three EAA states: Norway, Iceland and Liechtenstein.

Consequently, for the purpose of this deliverable, Norway should not be seen as a non-EU country from which data can be transferred to an EU-country but should rather be seen as a country that is part of the EU single market and as such governed by the GDPR.

As part of the European Economic Area, Norway is bound by the GDPR, which resulted in the adoption of a new Privacy Act and other legislative changes to comply with the new data protection rules. The Act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.

In preparation for the GDPR, large areas of Norwegian law underwent a thorough review, and legislative changes were made as needed. This included the implementation of a new Privacy Act, and technical changes in the legislation relating to camera monitoring in the workplace and access to employees' emails. The Privacy Act section 6 (the equivalent of GDPR article 88(1)) give employers the right to process special categories of personal data if it is necessary for carrying out the employer or employee's obligations or rights in the employment field.[4]

For these reasons, any transfer of personal data from the Norwegian beneficiaries (SINTEF and TELLU) should be assessed in light of the GDPR and should thus be discussed in the context of D8.1, D8.2, D8.3 deliverables and Chapter 3 of the present deliverable.

5.2 United Kingdom (UK)

The GDPR is retained in domestic law as the UK GDPR[5], but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018[6]. The key principles, rights and obligations remain the same with the core EU GDPR.

Data Protection Representative (DPR)

Because the UK GDPR has an extraterritorial scope, just like the original GDPR, this means that if you are an organization transferring personal data from the United Kingdom to Europe or vice versa you will have to appoint a data protection representative. This position can be fulfilled by a legal or natural person. It is important to know what a DPR does. The DPR has insight and access to the details regarding the processing of personal data that is carried out on individuals in Europe or the United Kingdom by your organization. Meaning that the DPR needs to have access to the organization's overview of personal data that is being processed. In the GDPR this is called the 'record of processing activities'. Next to that, the DPR needs to have access to relevant procedures within the organization to act in its capacity as the official representative. For example, when an individual informs the DPR that he or she wants to

[4] Third Countries - General Data Protection Regulation (GDPR) (gdpr-info.eu)

[5] https://uk-gdpr.org/

[6] The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

receive a copy of the personal data that is being processed by your organization, the DPR needs to be able to help the data subject with that request. While the responsibility of the processing activity remains with the organization (also called the controller), the DPR can be held liable for how he or she carries out this role for the organization. This means that the DPR can be subject to enforcement procedures by the ICO or European supervisory authorities.

Transferring personal data from the European Union to the United Kingdom or vice versa

Currently, the United Kingdom is a third country under the GDPR. This means that data transfers to the United Kingdom are restricted unless the United Kingdom receives an adequacy decision from the European Union. Restricted means normal transfer operations are not allowed, and to still transfer personal data to the United Kingdom a derogation in the GDPR will need to be used. These can be standard contractual clauses (SCCs), binding corporate rules or a one-off derogation such as informed and explicit consent by the data subject. In practice this means that an existing data processing agreement you might have with, for example, an IT firm in the United Kingdom will no longer be in effect, and one of these other transfer mechanisms needs to be used. It is recommended to gain insight into which data flows there are from the European Union to the United Kingdom and to subsequently update the transfer mechanisms as soon as possible to escape liability under the GDPR.

IDIADA UK is a linked third party connected with IDIADA SP. Obviously both entities follow the rules laid out in the UK and EU GDPRs and any other relevant data protection legislation concerning the transfer of personal data between them. A DPR is appointed at IDIADA UK to monitor compliance in the transfer of data for the UK side. A DPO is appointed at IDIADA SP to ensure that the organisation processes the personal data of its staff, customers, providers, or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. Finally, IDIADA UK and IDIADA SP respect a common group-level data protection policy safeguarding the transfer of data between them.

6 Analysis of data processing activities in ERATOSTHENES involving non-EU countries.

Research activities in ERATOSTHENES project that qualify as research in non-EU countries will be conducted in the IDIADA (UK), SINTEF (NO) and TELLU (NO)

The activities that will be conducted at the beneficiaries within the project framework include:

1. Field studies/pilots involving employees from IDIADA, SINTEF and TELLU. These studies/pilots will comply with the procedures as described in D8.1, D8.2 and D8.3. and Chapter 3 in the present deliverable (consent forms, data anonymisation, etc).
2. Interviews with stakeholders/employees in UK and Norway. These activities will fully comply with the procedures as presented in D8.1, D8.2 and D8.3. and Chapter 3 in the present deliverable (consent forms, data anonymisation, etc).
3. Laboratory test in IDIADA, SINTEF and TELLU, using local equipment and opensource software. These tests will fully comply with the procedures as described in D8.1, D8.2 and D8.3. and Chapter 3 in the present deliverable (consent forms, data anonymisation, etc).
4. Production of documents, reports, and scientific papers. These activities do not raise specific ethics issues.
5. Organization and hosting of workshops and training events. These activities will fully comply with the overall procedures and commitments related to the protection of personal data (as described in detail in D8.1, D8.2 and D8.3. and Chapter 3 in the present deliverable).

In particular, the research activities undertaken by IDIADA, SINTEF and TELLU, will be limited to software development as described in T2.3, 2.4, 2.5, 5.4 and 5.6. The software will be tested on TELLU's healthcare pilot, but only focused on the identity and access control mechanisms, rather than the patient monitoring features. Therefore, ***we will not collect, analyse or store any personal data from real patients, whereas only use artificial/anonymised data for testing. There will not be any issue related to exporting or importing personal data. The software will be open-sourced, and thus also no issue for import or export of software.*** In case activities undertaken in Norway raise ethics issues, the applicants will ensure that the research conducted there will be legal in at least one EU Member State.

As confirmed by IDIADA, SINTEF and TELLU all the aforementioned activities will fully comply with the higher standards of research integrity as stated in the regulations concerning scientific/data integrity of the GDPR. Furthermore, those activities that will be performed in the UK and Norway are legal in any EU Member State. There will be zero material transfer across EU borders. Data will only be shared for common publications and reports according to good scientific practice.

7 Conclusions

From the above chapters it is evident that ***only anonymous data will be processed***. Furthermore, it appeared that the laws that govern the non- EU repositories involved in ERATOSTHENES only apply to processing activities and transfer of data that concern identifiable information.

Consequently, it can be concluded that the processing activities carried out in the project are not subject to the national data protection laws of the countries in which the non-EU companies are located and that, to our current understanding, ***there are currently no requirements that should be complied with data stored in the non-EU beneficiaries to be transferred to the EU or another third country.***

Nevertheless, the consortium is aware that the assessment of the identifiability of the genetic data concerned is a dynamic exercise which cannot be decided upon once and for all. The beneficiaries therefore commit to periodically re-assess the risk of re-identification at every stage of processing and to further investigate any national guidance on anonymisation of information for research purposes.

Should it at a further stage become clear that the processing activities carried out in the research project do involve identifiable information in the sense of the relevant national data protection laws, then the beneficiaries ascertain that the requirements of those laws will be analysed on a more thorough level, to guarantee strict compliance.

That is why the technically skilled beneficiaries of the project will monitor the data processing activities performed in the project and will report on any changes thereof to the legal and ethics partners involved in ERATOSTHENES. This will allow ERATOSTHENES consortium to re-assess its current compliance whenever necessary, to remain compliant throughout the entire project.