
# 5G ExPerimentation Infrastructure hosting Cloud-nativE Netapps for public proTection and disaster RElief

Innovation Action – ICT-41-2020 - 5G PPP – 5G

Innovations for verticals with third party services

# D7.5: Data Privacy Impact Assessment preliminary version

Delivery date: August 2022

Dissemination level: Public

| | |
|---|---|
| **Project Title:** | **5G-EPICENTRE - 5G ExPerimentation Infrastructure hosting Cloud-nativE Netapps for public proTection and disaster RElief** |
| **Duration:** | **1 January 2021 – 31 December 2023** |
| **Project URL** | https://www.5gepicentre.eu/ |

This project has received funding from the European Union's Horizon 2020 Innovation Action programme under Grant Agreement No 101016521.

# Document Information

| Deliverable | D7.5: Data Privacy Impact Assessment preliminary version |
|---|---|
| **Work Package** | WP7: Project Management |
| **Task(s)** | T7.3: Legal framework and ethical supervision |
| **Type** | Report |
| **Dissemination Level** | Public |
| **Due Date** | M20, August 31, 2022 |
| **Submission Date** | M20, August 31, 2022 |
| **Document Lead** | Yerasimos Yerasimou (EBOS) |
| **Contributors** | Christos Skoufis (EBOS) |
| **Internal Review** | Laurent Drouglazet (ADS)<br>Kirsten Krüger (HHI)<br>Holger Gäbler (HHI)<br>Ankur Gupta (HHI) |

# Document history

| Version | Date | Changes | Contributor(s) |
|---|---|---|---|
| V0.1 | 06/60/2022 | Initial deliverable structure | Yerasimos Yerasimou (EBOS) |
| V0.2 | 01/07/2022 | 50% of the deliverable content | Yerasimos Yerasimou (EBOS) |
| V0.3 | 23/07/2022 | Input from DPIA questionnaires received | Yerasimos Yerasimou (EBOS) |
| V0.4 | 02/08/2022 | 90% of the deliverable content | Yerasimos Yerasimou (EBOS)<br>Christos Skoufis (EBOS) |
| V1.0 | 12/08/2022 | Internal Review Version | Yerasimos Yerasimou (EBOS) |
| V1.1 | 19/08/2022 | 1st version with suggested revisions | Kirsten Krüger (HHI)<br>Holger Gäbler (HHI)<br>Ankur Gupta (HHI) |
| V1.2 | 24/08/2022 | 2nd version with suggested revisions | Laurent Drouglazet (ADS) |
| V1.5 | 29/08/2022 | Final Version for Quality & Security Review | Yerasimos Yerasimou (EBOS) |
| V1.6 | 31/08/2022 | First revisions after final review | Yerasimos Yerasimou (EBOS) |
| V2.0 | 31/08/2022 | Final version for submission | Yerasimos Yerasimou (EBOS) |

## Project Partners

| Logo | Partner | Country | Short name |
|---|---|---|---|
| | AIRBUS DS SLC | France | **ADS** |
| | NOVA TELECOMMUNICATIONS SINGLE MEMBER S.A | Greece | **NOVA** |
| | Altice Labs SA | Portugal | **ALB** |
| | Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. | Germany | **HHI** |
| | Foundation for Research and Technology Hellas | Greece | **FORTH** |
| | Universidad de Malaga | Spain | **UMA** |
| | Centre Tecnològic de Telecomunicacions de Cata-lunya | Spain | **CTTC** |
| | Istella SpA | Italy | **IST** |
| | One Source Consultoria Informatica LDA | Portugal | **ONE** |
| | Iquadrat Informatica SL | Spain | **IQU** |
| | Nemergent Solutions S.L. | Spain | **NEM** |
| | EBOS Technologies Limited | Cyprus | **EBOS** |
| | Athonet SRL | Italy | **ATH** |
| | RedZinc Services Limited | Ireland | **RZ** |
| | OptoPrecision GmbH | Germany | **OPTO** |
| | Youbiquo SRL | Italy | **YBQ** |
| | ORamaVR SA | Switzerland | **ORAMA** |

# List of abbreviations

| Abbreviation | Definition |
|---|---|
| **AR** | Augmented Reality |
| **DMP** | Data Management Plan |
| **DMZ** | Demilitarized Zone |
| **DoA** | Description of the Action |
| **DPIA** | Data Protection Impact Assessment |
| **DPO** | Data Protection Officer |
| **EB** | Ethics Board |
| **EC** | European Commission |
| **ePD** | e-Privacy Directive |
| **ePR** | e-Privacy Regulation |
| **EU** | European Union |
| **GA** | Grant Agreement |
| **GDPR** | General Data Protection Regulation |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **ICT** | Information and Communication Technology |
| **NDA** | Non-Disclosure Agreement |
| **NetApp** | Network Application |
| **PPDR** | Public Protection and Disaster Relief |
| **QoE** | Quality of Experience |
| **RBAC** | Role-Based Access Control |
| **TLS** | Transport Layer Security |

| | |
|---|---|
| **UC** | Use Case |
| **VM** | Virtual Machine |
| **WP** | Work Package |

# Executive summary

This document presents D7.5 “Data Privacy Impact Assessment preliminary version” and responds to the Subtask 7.3.1 “Ethical oversight, validation and updates” in Task T7.3 “Legal framework and ethical supervision” under Work Package (WP) 7 “Project Management”. This report is a “living” document. Its initial version is reported in this deliverable, where a preliminary Data Protection Impact Assessment (DPIA) has been performed, to identify any legal and ethical requirements for the project activities and propose mitigation measures. Moreover, an overview of the legal and ethical framework to which 5G-EPICENTRE adheres is provided. Finally, the activities involving ethical aspects within the project are reported.

In this deliverable, the initial version of the DPIA is provided based on the input received by all consortium partners following the work done in the first half of the project in D7.8 “Data management plan second version”. The final version of the DPIA will be reported in D7.6 “Data Privacy Impact Assessment final version”, which is due in M36.

# Table of Contents

# List of Figures

# List of Tables

# 1 Introduction

5G-EPICENTRE aims to provide a platform for 5G experimentation to Network Application (NetApp) developers and other interested Information and Communication Technology (ICT) stakeholders, with the opportunity to test and evaluate their services and/or products for the Public Protection and Disaster Relief (PPDR) sector. The platform will offer testing of the services on a federated 5G infrastructure, consisting of testbeds in four different locations (Málaga, Aveiro, Barcelona, and Berlin). In order to achieve this vision successfully, a wide range of research activities are planned for testing, evaluating, and demonstrating the 5G-EPICENTRE system (or some selected features), including the realisation of eight Use Cases (UCs) and the organisation and execution of a hackathon for third-party developers. As these activities require the participation of humans and, in some cases, the processing of their personal data, the consortium should have mechanisms in place to safeguard the operating framework which is imposed by the European Commission (EC) and that all reasonable mitigation measures have been applied. One of the non-functional requirements of the platform, as these have been documented in D1.3 "Experimentation requirements and architecture specification preliminary version", is that the system must be privacy-compliant (NFR3). Thus, all the actions taken to ensure compliance to the NFR3 are reported in this deliverable. This document is structured as follows:

- Section 2 provides an insight into the legal and ethical framework to which 5G-EPICENTRE consortium should adhere.
- Section 3 provides an overview of the activities which are undertaken in this project and which include ethical aspects.
- Section 4 provides the initial version of the DPIA, which was completed in M19.
- Section 5 concludes this report and provides information for the future of this work.

## 1.1 Mapping of project's outputs

The purpose of this section is to map 5G-EPICENTRE 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 5G-EPICENTRE's GA Deliverable & Tasks Descriptions

| 5G-EPICENTRE Task | Respective Document Chapters | Justification |
|---|---|---|
| T7.3.1: Ethical oversight, validation and updates<br>"*In this sub-Task, the Ethics Manager, in close collaboration with the technical partners responsible for defining the platform architecture and developing the platform technologies, will guide and assess the integration of the legal and ethical requirements in the design of the platform.*<br>*As the technological development of the project evolves, this Task will: i) provide oversight and guidance on the implementation of the legal and ethical requirements in* | 2 - Legal and ethical framework | Section 2 presents the legal and ethical framework imposed by the EC to which the project adheres. |

| | | |
|---|---|---|
| *the pursuit of an ethically and legally compliant development that safeguards the privacy and data protection of individuals involved in the use case scenarios;"* | | |
| T7.3.1: Ethical oversight, validation and updates<br><br>*"iii) develop a Data Privacy Impact Assessment (DPIA) in accordance with the GDPR, to identify potential legal and ethical threats raised by the use of the technology and provide guidance concerning the measures, safeguards and mechanisms needed for the protection of personal data;"*<br><br>*"A key result of this Task is the DPIA, which is concerned with the implementation of a comprehensive privacy and ethical impact assessment to mitigate the impact of 5G-EPICENTRE on privacy and other fundamental rights and ethical values. It will include an assessment of the impact of the system and its modules on privacy and other fundamental rights from legal and ethical perspectives and finding ways to mitigate or avoid any adverse effects. To conduct this DPIA, all the consortium members will engage in a collaborative exercise, which can be done through activities such as questionnaires, teleconferences and interviews of the legal and ethics partners with the different stakeholders involved (technical partners and end-users) with the goals of (1) refining the initial analysis and (2) identifying the most adequate mitigation measures. Then, an identification of the ethical and legal risks posed by 5G-EPICENTRE and the most frequently adopted mitigation measures, will be conducted. This collaboration will* | 3 - Activities of 5G-EPICENTRE involving ethical aspects | In this section the activities and actions taken by the Ethics Board (EB) in accordance with the framework presented in Section 2 are presented. |
| | 4 - Data Protection Impact Assessment | In this section the initial version of the DPIA is provided, The DPIA includes input from all the partners who process data within the scope of 5G-EPICENTRE. |

| | | |
|---|---|---|
| *serve as a platform for a dialogue between all the partners involved in the project with the common goal to ensure that the final product meets ethical and legal standards. The results will be discussed and explained in project meetings and internal workshops, to select the most appropriate and relevant mitigation measures."* | | |

# 2 Legal and ethical framework

The legal and ethical framework related to the activities envisioned in 5G-EPICENTRE is presented in the following sections, as these are imposed by the European Union (EU) and national regulations of the participating countries. Although the ethics of the project are heavily based on the compliance with the General Data Protection Regulation (GDPR) [1], other regulations such as the e-Privacy Directive (ePD) and Free Flow of Non-Personal Data Regulation are considered.

## 2.1 General Data Protection Regulation

The GDPR (2016/679) is an EU law regulation concerning data protection and privacy, which is applicable in both the EU and the European Economic Area, while actions in the event of transferring personal data outside those regions are considered. Based on the DPIA presented in Section 4, transfer of any data outside the regions specified in the GDPR is not foreseen throughout the project's activities.

Through GDPR, a specific framework of obligations is imposed on both controllers and processors, in an unambiguous way, compared to the previously existing directives and regulations. In particular, the GDPR regulation replaces the Data Protection Directive 95/46/EC; and its main purpose is to provide individuals with controls and rights over their own personal data. The GDPR is directly binding and applicable, as it is a regulation and not a directive. Within GDPR (Article 4[1]), a wide range of legal terms and definitions is documented. Nonetheless, this report deals with the most relevant terms to the project's activities and overall scope, whose definitions are provided:

- **Personal data:** Is deemed as any information related to an identified or identifiable individual. Examples personal data are (but not limited to) the individual's name, residence address, email address, gender, ethnicity, religion, biometric information.
- **Data processing:** Overall, data processing is considered as any action that is performed on the personal data regardless of the action being automated or not. Such actions include collection, organisation, storage, use and alteration of data.
- **Data subject:** The data subject is the individual, whose own data is processed.
- **Data controller:** The data controller can either be a natural or legal person, a public authority, an agency or any other body. The data controller is the one who determines the purposes and mean of the processing of personal data, either alone or in collaboration with other entities.
- **Data processor:** The data processor is a third party who processes the personal data of individuals on behalf of the data controller.

The complete privacy policy to which 5G-EPICENTRE adheres is available on the project website[2].

### 2.1.1 Sensitive personal data

Under GDPR, a dedicated category of personal data is included, identified as *"sensitive personal data"*. This type of data must be treated with additional security and therefore, cannot be processed under the same procedures utilised for the rest of personal data. Such data requires specific processing conditions. According to Article 4 (13), (14), (15) and Article 9[3] of the GDPR, personal data that are considered sensitive are:

a. Personal data that include racial or ethnic origin of the subject, its political opinions, as well as its religious or philosophical beliefs;

[1] Art. 4 GDPR - Definitions - GDPR.eu
[2] https://www.5gepicentre.eu/privacy-policy/
[3] Art. 9 GDPR - Processing of special categories of personal data- GDPR.eu

b. Trade-union membership;
c. Personal data that reveal genetic data or biometric data processed in order to reveal the identity of a human being;
d. Personal data related to the subject's health; and
e. Data about the sexual orientation or the sex life of the subject.

As it is further elaborated in Section 4, through 5G-EPICENTRE research activities, biometric data are collected. Nonetheless, these are not classified as personal data, as the processing purpose is not for the identification of individuals.

### 2.1.2 Data processing

Under GDPR, the partners of 5G-EPICENTRE are only able to collect, use, store or sell any personal data if at least one of the conditions specified in Article 6[4] (1) is satisfied. In particular, one of the following conditions must be met:

a. Consent for the processing of their personal data for one or more specific purposes has been received by the data subject.
b. The processing of the personal data is necessary for the execution of a contract, in which the data subject is a party.
c. Processing is necessary in order to comply with legal obligations to which the data controller is the subject.
d. The processing is required to protect the vital interests of the data subject or of another natural person.
e. Processing is necessary for the performance of an action that will safeguard the public interest or in the exercise of official authorities vested in the data controller.
f. The processing of data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Cases in which the interests or fundamental rights and freedoms of the data subject require protection of personal data, and particularly when the data subject is a child, such condition does not apply.

If any of the aforementioned conditions are met and, thus, the lawful basis for data processing has been established, the data controller can proceed with processing of data, whereas the data subject is notified, thus ensuring compliance with the particularities of data transparency. Any change in the legal basis for processing requires the data controller to document the changes and inform the data subjects.

Partners of 5G-EPICENTRE process data only in the event of receiving a signed consent form by the data subject, that allows them to process their personal data for the specific purposes of the project that are clearly stated on the accompanied information sheet.

In Article 5[5] of the GDPR, the principles that should be considered for ensuring protection when processing data are provided and are listed below:

1. **Lawfulness, fairness, and transparency:** The processing of data is conducted within a lawful, fair and transparent framework regarding the data subject.
2. **Purpose limitation:** The data is collected for specified, explicit, and legitimate purposes. To this end, further processing for archiving purposes in the public interest, scientific or historical research purposes

[4] Art. 6 GDPR – Lawfulness of processing - GDPR.eu
[5] Art. 5 GDPR - Principles relating to processing of personal data - GDPR.eu

or statistical purposes shall be compatible with the initial purposes of collecting the data, in accordance with Article 89[6] (1) of the GDPR.

3. **Data minimisation:** The data shall be adequate, relevant and limited to what is necessary for the purposes for which they are being processed.
4. **Accuracy:** The data shall be accurate and, if relevant, kept up to date. Thus, every reasonable step must be taken in order to ensure that inaccurate personal data that are linked to the processing purposes are either erased or rectified without any delay.
5. **Storage limitation:** Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Therefore, personal data may be stored for longer periods, if they are processed solely for archiving purposes in the public interest; scientific or historical research purposes; or statistical purposes, in accordance with Article 89 (1) of GDPR. The aforementioned is subject to the implementation of the appropriate technical and organisational measures required by Article 5 of the GDPR in order to safeguard the rights and freedoms of the data subject.
6. **Integrity and confidentiality:** Appropriate security of the personal data is ensured during its processing, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate, technical, or organisational measures.
7. **Accountability:** The data controller shall be responsible for compliance with points (1)-(6); and be able to demonstrate the same.

Based on these conditions, the data management plan (DMP) is addressing these points by providing relevant questions to the partners who are processing (or foresee to process) data, in the framework of the project. The DMP was reported in M4 (D7.7); and was updated in M18 (D7.8).

Thus, through this exercise, adherence to the restrictions is achieved. Some examples include (but not limited to) the clarification by partners as to the purpose of collecting data, as well as which data and to what extent, which relates to point (2): Purpose limitation. Moreover, partners are asked to state the retention period for the processed data, in order to ensure that (5): Storage limitation is adhered to. Finally, another example is the use of consent forms and information sheet before processing any data, which is linked to condition (1): Lawfulness, fairness, and transparency.

### 2.1.3 Rights of data subjects

In general, human participants involved in research activities are entitled to several rights with respect to the processing of their personal data. The introduction of the GDPR aided in the enrichment of existing rights of data subjects, as these were defined in the Data Protection Directive (Directive 95/46/EC) [2], whereas it introduced new rights that aimed in covering the gaps created in the existing legal and ethical framework. To this end, it is essential that the 5G-EPICENTRE consortium is aware of the research participants' rights; and ensure adherence to them by taking all the necessary actions. Under the GDPR (Articles 15–22), the human participants have the following rights [3]:

a. The data subject's right of access.
b. The data subject's right to rectification.
c. The right to erasure (or to be forgotten).
d. The data subject's right to restriction of processing.
e. The right to be informed.
f. The right to data portability.
g. The right to object.

[6] Art. 89 GDPR - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes- GDPR.eu

h. The right to not be subject to a decision based only on an automated processing.

As indicated in the templates of the informed consent forms (provided in Annex I), before any data is being collected, the data subject must sign the forms and provide her/his consent. It should be noted that all human participants have the right to withdraw their consent at any point without being required to justify their choice. In such case, their data will be immediately deleted unless there is a legal basis and contractual obligation to be preserved.

### 2.1.4 Data Protection Impact Assessment

According to Article 35[7] of the GDPR, a DPIA[8] is required in cases where the rights and freedoms of data subjects are likely to be under high risks through the processing of their data. In particular, a DPIA is required if any of the following applies:

a. An automated decision making, such as profiling, for a systematic and extensive evaluation is applied to the personal data related to natural persons.
b. An extensive processing of sensitive data occurs.
c. A systematic monitoring of public areas occurs on a large scale.

Based on the latest version of the DMP (D7.8), 5G-EPICENTRE does not require a DPIA at this phase, as none of the aforementioned conditions are met. As shown in Section 4, there are cases where biometric data will be collected for the execution of UC8, which fall under the category of "sensitive personal data". However, this action is not characterised as an "*extensive processing of sensitive personal data*". In addition, for UC7 it is envisioned that footage and Global Positioning System (GPS) location will be captured by wearable devices, which is not considered as "*systematic monitoring of public areas on a large scale*".

Nonetheless, even though a DPIA is not strictly mandatory for fulfilling the project purposes, it remains a good practice and a useful tool for data controllers in complying with the GDPR [1].

### 2.1.5 Data anonymisation

For numerous EU legislations and directives, including the GDPR, anonymisation of data is considered as an effective measure for preventing data subjects' identification. Through data anonymization, all private and sensitive information of data subjects are either completely erased, or replaced by encrypted identifiers that connect the individual subject to its data. This is a necessary measure that shall be taken, even if there is a legal basis to process the personal data identified in accordance with Articles 5 and 6 of the GDPR.

In this regard, several key aspects shall be considered when applying such techniques. As data anonymisation requires assurance with respect to the satisfaction of the necessity of compatibility by having regard to the legal grounds and circumstances of the further processing, it is a more complicated procedure than just the process of personal data. Some of the most prevalent anonymisation methods are data masking, generalisation and data swapping. Data masking is a method in which the data is hidden with replaced values, by utilising techniques such as encryption, character or word replacement, and character shuffling. Generalisation can be used by removing certain identifiers in a dataset, in order to make it more general. Finally, data swapping is a method where values in the dataset are swapped, aiming at having data values that do not correspond to the initial dataset.

Pseudonymisation, on the other hand, is a method that can be employed by having some data protection while preserving the integrity of the original data and the statistical accuracy, through the replacement of unique identifiers with fake ones or pseudonyms. Despite the many advantages this method offers, it cannot be used solely

[7] Art. 35 GDPR - Data protection impact assessment- GDPR.eu
[8] In the GA, Data Protection Impact Assessment is referred to as Data Privacy Impact Assessment.

as an anonymisation technique. This is due to the fact that although pseudonymisation reduces the link between the original and modified datasets, such connections are not fully eliminated. As stated in Recitals 28 and 29 of the GDPR:

- The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of "pseudonymisation" in this Regulation is not intended to preclude any other measures of data protection. (Recital 28)
- In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller, when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller. (Recital 29)

In general, a combination of the aforementioned methods yields the most effective results for data anonymisation. However, it should be highlighted that even though a combination of techniques could be applied, there are residual risks, as de-anonymisation can be applied; a method where the anonymised data is cross-referenced with other databases, thus aiming at the re-identification of data subjects. 5G-EPICENTRE, in order to ensure that risks are mitigated, will follow data minimisation principles to prevent individuals from being able to trace research participants and link them to a specific UC demonstration, or the Hackathon event.

The project complies with the GDPR and any local legislation (if required). To this end, specific measures have been set if personal data is exchanged between the consortium partners. In particular, full anonymisation is required prior sharing personal data between partners. It is possible that data is exchanged among partners without being fully anonymised, if this is required for the purposes of the project. In this case, the specific partners shall conduct a separate agreement for data processing, thus setting their own operational measures to be taken prior to the exchange or processing. It should be noted that despite separate agreements, the data exchange measures must be in accordance with the EU Data Protection Legislation.

## 2.2 e-Privacy Directive

The Directive 2002/58/EC on privacy and electronic communications as ePD was amended by Directive 2009/13631; and they were transposed into EU nations' laws [5]. Their scope is to protect privacy in the electronic communications sector (*e.g.*, communications metadata) and they can complement the GDPR on electronic communications privacy. The 5G-EPICENTRE project will follow the ePD.

The e-Privacy Regulation (ePR) [6], which is not in force, is set to repeal the current Directive. Unlike the Directive, the Regulation is a legal act of the EU, thus forcing all state members to abide by it effective immediately. The latest update of the ePR is the derogation approved by the European Parliament on 06/07/2021, allowing electronic communication providers to seek and report material related to child sex abuse in private conversations.

## 2.3 Free flow of non-personal data

The Regulation of the Free Flow of Non-Personal Data [7] was introduced in 2018. Its main aim is to limit the complications regarding the free flow of data in the EU. Operating in conjunction with the GDPR, whose purpose is to protect personal data, this Regulation has been adopted for ensuring the free flow of non-personal data, thus boosting the digital single market. The tools for achieving its objectives include forbidding localisation requirements for mandatory data, unrestricted access to competent authorities to such data, and facilitation of data porting by users.

Non-personal data is defined in the Regulation as the data that is not personal, by the definition of personal data that is provided in Article 4(1) of the GDPR. Consequently, non-personal data is considered as all data that is not classified as personal.

# 3 Activities of 5G-EPICENTRE involving ethical aspects

The activities of the project envisage the involvement of human participants throughout the UC execution, as well as during the hackathon. To this end, actions have been defined and implemented to safeguard the privacy and protection of human participants and to ensure that the consortium is operating under the ethical framework imposed by the EU.

## 3.1 Ethics Board

Ethical oversight is provided via an Ethics Board (EB), that was formed by partners of the consortium. The EB has a supervisory role, and its main aim is to ensure that any actions related to the project's activities, including participation of humans in the UCs and hackathon event, are performed while adhering to the legal and ethical framework imposed by the EC, as these have been defined in Section 2. The EB meets on an ad-hoc basis, whenever deemed necessary by any of its members. The main objectives of the EB are the following:

- Supporting the consortium's activities by providing relevant information regarding Legal and Ethical regulations affecting the partners' actions
- Continuous monitoring and updating of the DMP in the event new data are required for the project activities;
- Identification of events or other project activities that could potentially entail ethical risks;
- Continuous monitoring of the partners' activities and ensuring that their actions are adhering to the Legal and Ethical framework;
- Analysis of the information provided in the DPIA and decision on the mitigation measures to minimise any potential risks.

The EB has a monitoring role for the duration of the project. To this end, the EB provides continuous review of material produced by the consortium, including deliverables, dissemination material, press releases etc., in order to prevent any actions that could compromise the project from a legal and/or ethical standpoint. In general, identification of risks and monitoring of new and existing project activities by the EB are an ongoing process that is active throughout the project's lifespan. It should be noted that any decisions or recommendations of the EB, as well as relevant action points, are communicated to the consortium.

The individuals forming the EB of 5G-EPICENTRE and their respective role are provided in Table 2.

Table 2: Ethics Board members

| Name | Organisation | Role |
|---|---|---|
| Alain Dubois | ADS | Project Coordinator |
| Konstantinos Apostolakis | FORTH | Technical Manager |
| Yerasimos Yerasimou | EBOS | Ethics Manager |
| Ioannis Markopoulos | NOVA | Dissemination and Communication Manager |

## 3.2 Data Management Plan

The DMP of the project is a live registry, where partners report on their intention to process data within the framework of 5G-EPICENTRE's activities, as well as the procedures they follow in the event they do process data.

In the DMP there is a distinct classification between personal and other data, which helps in isolating data that require the attention of the EB. Two official releases of the DMP have been reported in D7.7 (M4, resubmitted M12) and D7.8 (M18), respectively. Moreover, partners who do process data are required to provide the contact details of their organisation's Data Protection Officer (DPO) and internal data processing policies[9].

## 3.3 Criteria in recruiting research participants

As mentioned earlier, 5G-EPICENTRE envisages the development of a federated platform for the testing of NetApps aimed at the PPDR sector. The objectives of the project, which will be realised through the deployment of eight UCs, involve activities such as gathering of requirements, lab testing, trial validation, user evaluation, as well as small-scale assessments by gathering users' input. All the aforementioned activities aim towards analysing and assessing the usability of the platform, technology acceptance and impact creation. Therefore, humans, including volunteers, may participate in the predefined UC environments. It should be noted that the consortium partners devote efforts in mobilising relevant user groups, such as public safety organisations and first responders, as well as policy makers and administration authorities, which helps in recruiting relevant users and stakeholders for the live demonstrations. More information about the target groups of the 5G-EPICENTRE is available in D6.2 "Plan for Using and Disseminating Knowledge year 2", also submitted in M20.

The project ensures that equal opportunities are provided regarding the participation in the UCs of the project. Moreover, discrimination on any forbidden grounds, such as age, sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or other opinion, membership of a national minority, property, sexual orientation and disability, is forbidden, thus abiding by Article 21 (Non-discrimination) of Equality [8].

In addition, the project makes every reasonable effort to avoid participants' exclusion from its envisaged activities for reasons such as the platform not being reasonably user-friendly, cultural bias propagated through the language used via the project's communication and promotion of certain societal communities.

## 3.4 Secondary data

Secondary data includes data that has been repurposed; and is therefore used in a different scope compared to the original purpose for which it was gathered. Unlike primary data, which refers to data collected by the project partners to fulfil the objectives of 5G-EPICENTRE, secondary data could also be processed, thus exploiting readily available data which may have been gathered for a different scope.

Although primary data is overseen by the ethics guidelines provided in this document, the ethics governing secondary data collection and/or processing depend on the terms and conditions of the original source, which have already been accepted by the subjects, *i.e.*, in case data is collected from a website, the terms and conditions that the user has accepted prior entering the website. To date, no need for secondary data has been identified by any of the consortium members.

## 3.5 Informed consent of research participants

As specified in Section 2.1.3, informed consent forms will be used before any data is collected from research participants that are involved in any research activity of the project that requires them to provide personal data. As such, the consent by all data subjects should be obtained by means in accordance with their age and competence level. The consent form will also be the means for obtaining voluntary participation to the activity. To this end, it is the responsibility of the partner representing 5G-EPICENTRE to provide the necessary information to any prospective participant, by adapting the information to their skill and needs with respect to readability and

[9] Information is available in D7.8.

visual appeal. Additionally, partners are able to redirect any prospective participant to the privacy policy of the project, which is available in the website.

Based on Article 7[10] of the GDPR, there are specific conditions to be met in order to have a valid consent for processing personal data. In particular [9]:

a. The consent must be freely given. Thus, the data subject must not be forced in any way to consent, even when being asked for their consent as a requirement for using a service.
b. The consent must be specific. Therefore, it should be clarified under which data processing activities their personal data will be used.
c. The consent must be informed; therefore, the prospective participant must be provided with information related to the processing activities that are intended to be applied and to their purpose.
d. The consent must be unambiguous. Specifically, the consent of the data subject must not be questionable in any way.
e. The consent must be revoked. Therefore, the participants have the right to withdraw their consent at any time.

The research objectives and expected outcomes of the project are communicated to the prospective participants in order to persuade them for joining the research activities, once they have provided their explicit consent to their personal data. In general, the actions to be followed for processing personal data are the following:

1. The consent form is digitised followed by destroying the hard copy. The soft copy is saved on a secure computer located at the premises of the designated data controller, in compliance with ISO/IEC 27001:2005 standards [10] concerning data security, aiming at safeguarding the data against accessibility by unwanted third parties or disaster.
2. Each participant is assigned a random index number, in the context of anonymisation procedures.
3. An encrypted file that is kept on a secure computer at the premises of the designated data controller includes all the relevant information for linking the digital consent form to the random index mentioned in (2).
4. All datasets are associated with the generated index, mentioned in (2).
5. Access to the encrypted file mentioned in (3) is only available to the designated data controller.

The aforementioned steps shall be followed for every activity of 5G-EPICENTRE that involves the collection, storage, and/or use of data. Once the processing period has expired, with a maximum time of five years after the project's completion, the data shall be deleted from all databases. Further processing of the data by some partners can be extended beyond the five years, if parallel legal obligation exists for such processing and therefore such legal basis is valid.

[10] Art. 7 GDPR – Conditions for consent - GDPR.eu

# 4 Data Protection Impact Assessment

A DPIA was conducted addressing the project partners that process data according to the DMP. The DPIA is based on the template provided in [11] and has the form of a questionnaire consisting of a set of questions, where the following are clarified:

- The aims of the activity under which data is processed and the type of processing - Table 3;
- The nature of the processing - Table 4;
- The scope of the processing - Table 5;
- The context of the processing - Table 6;
- The purpose of the processing - Table 7; and
- The compliance and proportionality measures - Table 8.

Table 3: DPIA – Aims of activity in which data is processed and type of processing

| **Explain the aims of the activity in which data is processed and what type of processing it involves.** | |
|---|---|
| **ADS** | Data is processed for the coordination of the project:<br>• Partners' email addresses and phone numbers are used for the project communication.<br>• Bank account details: Required for processing the project partners payments.<br>ADS does not process any special categories of personal data. |
| **NOVA** | Data is processed for receiving requirements responses according to the Description of the Action (DoA).<br>The responses will be used in the requirements collection process. Personal data will not be used and will be deleted following the requirements collection. |
| **ALB** | For ALB, data processing may be required in two types of activities:<br>• Hackathon preparation and management: Identification and contacts of participants; Other data to be processed will be defined during the preparation for the Hackathon within WP5.<br>• UC development: Identification and biometric data of UC participants/volunteers |
| **FORTH** | Data is processed for users that wish to use the experimental portal of 5G-EPICENTRE. |
| **YBQ** | YBQ processes data for the execution of UC7.<br>The smart-glasses worn by the PPDR practitioners are tracked through a GPS-enabled device, which is then communicated to the server application. The server organises the data in clusters and displays it on a geo- |

| | |
|---|---|
| | referenced map. Some devices in the field are put in video inter-communication with each other and can exchange text messages. |
| **ORAMA** | Regarding the UC8 led by ORAMA, the data processed are used:<br>• for user registration and login purposes (email addresses, full names, affiliation);<br>• for identifying potential issues and improve the application itself (questionnaires);<br>• for potentially providing a suitably translated user interface (country of origin); and<br>• to provide user analytics regarding their performance (personal score for each action within the application).<br>The credential data are processed during login to identify the user. The questionnaires are processed manually to identify issues on the performance of the application. The personal score for each action is processed via analytics engines. |

Table 4: DPIA – Nature of the processing

| **Describe the nature of the processing:** | |
|---|---|
| **How is the data collected, used, stored, deleted?** | |
| **ADS** | The email addresses, phone numbers and company bank accounts are sent by the partners via email. All data will be used only for the project purposes and deleted at the end of the project. |
| **NOVA** | Data is collected and used for the requirements for 5G-EPICENTRE. Personal data is deleted following the collection of requirements. |
| **ALB** | UCs: Monitoring probes deployed at the network and measurements provided by the system under test. Data is stored and processed.<br>Hackathon management: via enrolment web form<br>The policy for the deletion of the data is documented in Table 5. |
| **FORTH** | Data will be stored on a private server, accessible only through the internal network of the infrastructure. The connection between the users' browsers towards the private server will be encrypted using Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) connections.<br>The policy for the deletion of the data is documented in Table 5. |
| **YBQ** | We collect the data with GPS-enabled devices used in platform on the map and stored in database. Data can be deleted if requested. |

| | |
|---|---|
| **ORAMA** | Collection via the application itself:<br>• Credentials during registration and login sessions<br>• Questionnaires and personal score while using the application<br>The information is used for identifying a user (credentials), identifying issues on the performance of the application (questionnaires) and for providing analytics on the score of a user (personal score for each action within the application).<br>The data are stored anonymised in cloud storage (Azure).<br>The data are deleted upon request or at the end of the project or after the expiry date, as this has been reported in the DMP. |
| **What is the source of the data?** | |
| **ADS** | The data is sent by the partners. |
| **NOVA** | Surveys, Interviews |
| **ALB** | UCs: Monitoring probes<br>Hackathon management: enrolment web form |
| **FORTH** | Users will enter the information via the Portal front-end, served via a virtual machine (VM) of the demilitarized zone (DMZ). |
| **YBQ** | Smart glasses and other devices that produce the GPS information |
| **ORAMA** | Data originate from the users and their actions while using the application. |
| **Will you be sharing data with anyone?** | |
| **ADS** | No. |
| **NOVA** | No. |
| **ALB** | Data will not be shared with anyone outside the consortium. Results obtained will be aggregated or anonymized; whatever is considered more suitable. For Hackathon management, only partners involved in Task 5.2 will be granted access to participants' personal data. |
| **FORTH** | No. |
| **YBQ** | Only with partners of consortium that are relevant to UC7. |
| **ORAMA** | No. |
| **Which types of processing[11] are identified as high-risk?** | |

[11] Processing of data includes either collecting, using, storing or deleting data.

| | |
|---|---|
| **ADS** | None. |
| **NOVA** | None. |
| **ALB** | None. Any personal data, including biometric data, if needed for the implementation of any specific UC, will be anonymized. The collected data will only be relevant in the scope of the said UC. |
| **FORTH** | None. |
| **YBQ** | None. |
| **ORAMA** | None. |

Table 5: DPIA – Scope of the processing

| **Describe the scope of the processing:** | |
|---|---|
| **What type of data is collected?** | |
| **ADS** | Email, company bank accounts |
| **NOVA** | Email addresses, phone numbers, affiliation, position, research notes, interviews, questionnaires |
| **ALB** | UCs: Identification and biometric data.<br>Hackathon management: participants' identification and contacts |
| **FORTH** | E-mail addresses and other potential data (such as potentially organisational data for identifying/validating Portal roles [*e.g.*, testbed owners]; country of origin [for geo-blocking of blacklisted countries]; organisation VAT information [for asserting country of origin], *etc.*) will be used as part of the account setup for using the 5G-EPICENTRE Portal. In addition, agreement to terms and conditions will be a necessary step to allow signing up a new user account. |
| **YBQ** | GPS Position, Text messages, Email, Full names |
| **ORAMA** | Email addresses, full names, affiliation, questionnaires, country of origin, personal score for each action within the application. |
| **Does the data include special category[12] or criminal offence data?** | |
| **ADS** | No. |

[12] Please refer to Art. 9 GDPR for the definition of special category data: https://gdpr-info.eu/art-9-gdpr/

| | |
|---|---|
| **NOVA** | No. |
| **ALB** | UCs: Yes, biometric data, if needed for the implementation of any UC.<br>Hackathon management: No |
| **FORTH** | No. |
| **YBQ** | No. |
| **ORAMA** | No. |
| **How much data will be collected and used and how often?** | |
| **ADS** | The data is collected at the beginning of the project or if a new partner enters the project. |
| **NOVA** | The above-mentioned data will be collected from approximately 40 people, two times in the project's lifetime. |
| **ALB** | UCs: Data necessary for the deployment and testing of the defined UCs in ALB's testbed.<br>Hackathon management: Data necessary for participants' identification and contact |
| **FORTH** | Depending on the use of the platform, data relating to the partners' organisations with a direct stake in the 5G-EPICENTRE platform (*i.e.*, testbed owners and function developers/ experimenters) alongside participants to the Hackathon activities in the context of T5.2. All accounts will undergo an approval process prior to granting access to the Portal (*e.g.*, to make sure end-users will adhere to ethical or other special requirements coming from the EU). As many as 100 individual accounts are expected to be created during project lifetime activities. |
| **YBQ** | • GPS position: every 5 seconds<br>• Text message: every disaster event |
| **ORAMA** | • Email addresses, full names, affiliation, questionnaires, country of origin: on registration, once per user<br>• Personal score for each action within the application: on every session, per user, once per action (*e.g.*, if the user selects an option or triggers an action, it will be stored)<br>• Quality of experience (QoE) related questionnaire, after each session |
| **How long will the data be kept?** | |

| | |
|---|---|
| **ADS** | All data will be deleted at the end of the project. |
| **NOVA** | Personal data will not be used and will be deleted following the requirements collection. |
| **ALB** | UCs: Data will be kept in accordance with the data retention policy that will be agreed among the partners of the consortium.<br>Hackathon management: Participants' personal data will be kept until the project's conclusion and deleted immediately after. |
| **FORTH** | Data will be securely stored in a private server until 12 months after conclusion of the project. After this period, they will be deleted. We plan to indicate this in the Portal (*e.g.*, beta version) and the terms and conditions page where users will be notified of our intentions with the collected data. If exploitation plans foresee it, after moving to a new server (post-project exploitation by individual or groups of partners), new accounts will need to be registered, and the administrating entity will need to provide similar security mechanisms. |
| **YBQ** | The GPS position will be kept until the user requests deletion. |
| **ORAMA** | Until the end of the project or less, if the user requests the deletion of this data |
| **How many individuals are expected to be affected by the processing of data?** | |
| **ADS** | All the partners |
| **NOVA** | 40 people |
| **ALB** | It depends on the number of participants in the UCs. This also includes Hackathon participants; number is unknown at this point. |
| **FORTH** | Relating to the number of accounts approved |
| **YBQ** | Only technicians accessing the platform |
| **ORAMA** | The data of all users' actions will be processed by the analytics engine. |

Table 6: Context of the processing

| **Describe the context of the processing:** |
|---|
| **What is your relationship with the data subjects? (Research participants, partners of consortium, *etc.*)** |

| | |
|---|---|
| **ADS** | Project participants |
| **NOVA** | The data subjects are project's stakeholders. |
| **ALB** | UCs: partners of the consortium, volunteers<br>Hackathon management: Participants |
| **FORTH** | Users of the platform. Will include consortium members and Hackathon participants during project lifetime activities. |
| **YBQ** | Research participants and partners of consortium |
| **ORAMA** | Research participants, partners of consortium, PPDR volunteers |
| **How much control do the data subjects have over their personal data?** | |
| **ADS** | The partners control their data, it can be deleted by a mail request |
| **NOVA** | Questionnaire and interviews will have informed consent in the beginning. If the interviewee agrees, we will proceed.<br>Data subjects' request process, as defined in Articles 15-22 of the GDPR, describes how data subjects can freely exercise their rights through a corresponding application to be filled in on the Company's official communication channels. |
| **ALB** | Data subjects' control to be defined by the consortium (following D7.7, section 3.4) |
| **FORTH** | In accordance with principles of research ethics and EU data protection regulations, users will be fully informed about the purposes of data collection prior to creating their account. They will have the right to be informed about their personal data collected and to have access to them, and the right for these data to be in a portable and easily accessible form. They will also have the right to request that their personal data be corrected, updated or deleted, the right to have the processing restricted, and the right to object, with the reservation of any exceptions provided for in existing European and national legislation. |
| **YBQ** | Data subjects can control the data (delete the collected information upon request). |
| **ORAMA** | Complete control (able to view, alter, and delete them) |
| **Would the data subjects expect their data to be used in the way they are foreseen to be used by you?** | |
| **ADS** | Yes. |

| | |
|---|---|
| **NOVA** | Yes. |
| **ALB** | Yes. |
| **FORTH** | Yes, all use of the data will be elaborated in the Terms and Conditions page. |
| **YBQ** | Yes. |
| **ORAMA** | Yes. |
| **Are the data subjects children or other vulnerable groups?** | |
| **ADS** | No. |
| **NOVA** | No. |
| **ALB** | No. |
| **FORTH** | No. Age verification will be applied in the account creation process to ensure users are above the age of 18 when creating their account. |
| **YBQ** | It could happen that accidentally children or other vulnerable groups are in a video stream; however, their data will be anonymous. Moreover, video stream is not available publicly. |
| **ORAMA** | No. |
| **Are there prior concerns over this type of processing or security flaws?** | |
| **ADS** | No. |
| **NOVA** | No. |
| **ALB** | No. |
| **FORTH** | No. Data will be stored on a private server, accessible only through the internal network of the infrastructure. The connection between the users' browsers towards the private server will be encrypted using HTTPS and TLS connections. |
| **YBQ** | No. |
| **ORAMA** | No. |

Table 7: Purpose of the processing

| **Describe the purpose of the processing:** | |
|---|---|
| **What do you want to achieve through the processing of data?** | |
| **ADS** | Partner information used for project organisation and payments execution |
| **NOVA** | The responses will be used in the requirements collection process. Personal data will not be used and will be deleted following the requirements collection. |
| **ALB** | • UC roll out and demonstration (if data processing is required);<br>• Preparation of the Hackathon. |
| **FORTH** | Account creation on the Portal and use of the e-mail for login purposes. Ensuring the individual can be verified (*i.e.*, verification link sending to the e-mail account) and an appropriate role can be granted for role-based access control RBAC (*e.g.*, a third-party user cannot be assigned as a testbed owner). Also, ensuring that special requirements (*i.e.*, country of origin should not be blacklisted by EU services) are met prior to approving the account. |
| **YBQ** | Identification of devices (Augmented Reality [AR] smart glasses) position in order to broadcast alert messages |
| **ORAMA** | Identify users (credential related), provide user analytics (scores) and identify potential issues of the application (questionnaires). |
| **What is the intended effect on data subjects?** | |
| **ADS** | Not applicable. |
| **NOVA** | Not applicable. |
| **ALB** | None. |
| **FORTH** | Data subjects will be registered users of the Portal and should be able to log in to access the Portal services. |
| **YBQ** | Referral of the devices position on a geographical map. The device position data will not be linked to the personal data of the user. |

| | |
|---|---|
| **ORAMA** | They will be able to login (credentials) and they can identify where they performed well, throughout the user of the application. |
| **What are the benefits of the processing? (for your organisation, the project *etc.*)** | |
| **ADS** | Project administration. |
| **NOVA** | The elicitation of the requirements of the 5G-EPICENTRE platform. |
| **ALB** | Successful execution of the project activities and realisation of the intended project outcomes, as specified in 5G-EPICENTRE GA. |
| **FORTH** | Solid way for granting access to specific Portal services based on RBAC. Compliance to ethical requirements as identified in the project's Ethics Board meetings. |
| **YBQ** | Successful execution of the project activities relevant to UC7. |
| **ORAMA** | Potential improvement after identifying application issues. |

Table 8: DPIA – Compliance and proportionality measures.

| **Describe compliance and proportionality measures:** | | | | | |
|---|---|---|---|---|---|
| **What is the lawful basis for processing the data?** | | | | | |
| **ADS** | Not applicable. | | | | |
| **NOVA** | Internal policy of NOVA has been shared with the Ethics Manager. | | | | |
| **ALB** | Subjects informed consent (as per D7.7, section 3.7). | | | | |
| **FORTH** | Consent: The individual gives clear consent for the processing of the data for accessing Portal services. This will be facilitated with the individual being prompted to read and agree to the terms of service in order to complete their registration. | | | | |
| **YBQ** | EU GDPR | | | | |
| **ORAMA** | Data will be collected and processed after giving consent. | | | | |
| **Will the processing achieve the purpose of your activity?** | | | | | |
| **ADS** | Not applicable. | **NOVA** | Yes. | **ALB** | Yes. |
| **FORTH** | Yes. | **YBQ** | Yes. | **ORAMA** | Yes. |

| Is there an alternative way to achieve the same outcome? | | | | | |
|---|---|---|---|---|---|
| **ADS** | Not applicable. | **NOVA** | No. | **ALB** | No. |
| **FORTH** | No. | **YBQ** | No. | **ORAMA** | No. |

| How will you prevent function creep[13] of the processed data? | |
|---|---|
| **ADS** | Not applicable. |
| **NOVA** | The provisions for data security are described in the internal policy of NOVA.<br>The process of managing security incidents involving personal data includes identifying any data protection breaches, investigating the incident, and notifying the supervisory authority (and the subject, if this is required), if the breach is likely to pose a risk to the rights and the freedoms of natural persons. |
| **ALB** | Through the minimisation of the number of people with access to data and secure access |
| **FORTH** | Data will be stored on a private server, accessible only through the internal network of the infrastructure. Data will not be exposed by any means to third parties. |
| **YBQ** | The access to the app is locked. Any fraudulent action can be discovered. |
| **ORAMA** | Safe keeping of data in Azure, supervision of ORAMA's DPO |

| How is data quality and data minimisation ensured in the activity? | |
|---|---|
| **ADS** | Not applicable. |
| **NOVA** | The responses will be used in the requirements collection process. Personal data will not be used and will be deleted following the requirements collection. |
| **ALB** | The collected data will be as minimal as possible, if strictly required to enable the successful execution of the planned tasks. |
| **FORTH** | Only the data necessary for the purposes of the Portal's proper functionality will be collected. An approval procedure will be applied to ensure the accuracy, relevance, and completeness of data. |
| **YBQ** | Not applicable. |
| **ORAMA** | Minimal data are collected to serve the purposes mentioned. |

| What information is provided to the data subjects? (*e.g.*: consent form, information sheet, *etc.*) |
|---|

[13] Function creep is an outcome where results in data is being used for different purposes other than the ones the individual consented to or was told about upfront.

| | |
|---|---|
| **ADS** | Not applicable. |
| **NOVA** | Questionnaire and interviews will have informed consent in the beginning. If the interviewee agrees, we will proceed. |
| **ALB** | Information is provided as defined by the consortium, including consent form and information sheet. |
| **FORTH** | Terms of service, privacy policy |
| **YBQ** | Information is provided as defined by the consortium, including consent form and information sheet. |
| **ORAMA** | Data will be collected and processed after giving consent and reading the necessary information sheet. |
| **What measures are taken to ensure processors comply?** | |
| **ADS** | Not applicable. |
| **NOVA** | Questionnaire and interviews will have informed consent in the beginning. If the interviewee agrees, we will proceed. |
| **ALB** | • UCs: Data processing is only occurring by the involved consortium partners.<br>• Hackathon Management: Data processing is only occurring by the involved consortium partners. |
| **FORTH** | Data processors are FORTH employees working on the project. Technical and organizational measures will be applied, as described above, to ensure compliance with the European and national legislation on data protection and to protect data subject rights. |
| **YBQ** | Access to the data is only available to involved consortium partners. |
| **ORAMA** | Access to data is possible only by members of ORAMA who have signed the non-disclosure agreement (NDA). |
| **How are international transfers safeguarded? (transfer of data outside EU)** | |
| **ADS** | Not applicable. |
| **NOVA** | Internal policy of NOVA has been shared with the Ethics Manager. For the purposes of the project, no data transfers outside EU are required. |
| **ALB** | Not applicable. No international transfers will occur. |
| **FORTH** | No data will be transferred outside the EU. |

| | |
|---|---|
| **YBQ** | Not applicable. |
| **ORAMA** | No such transfer occurs. |

Based on the input received from the partners processing data a number of risks has been identified, as well as mitigation measures to limit their overall impact. As stated in Section 2.1.4, a DPIA is not necessary as per the definition provided in the GDPR; however, it was conducted to expose any potential ethical threads pertaining to the technical solution provided by 5G-EPICENTRE and the partners' activities. A simplified 3x3 risk assessment matrix was utilised for the classification of the identified risks, as these are listed in Table 9. In Figure 1, the risk assessment matrix is presented.

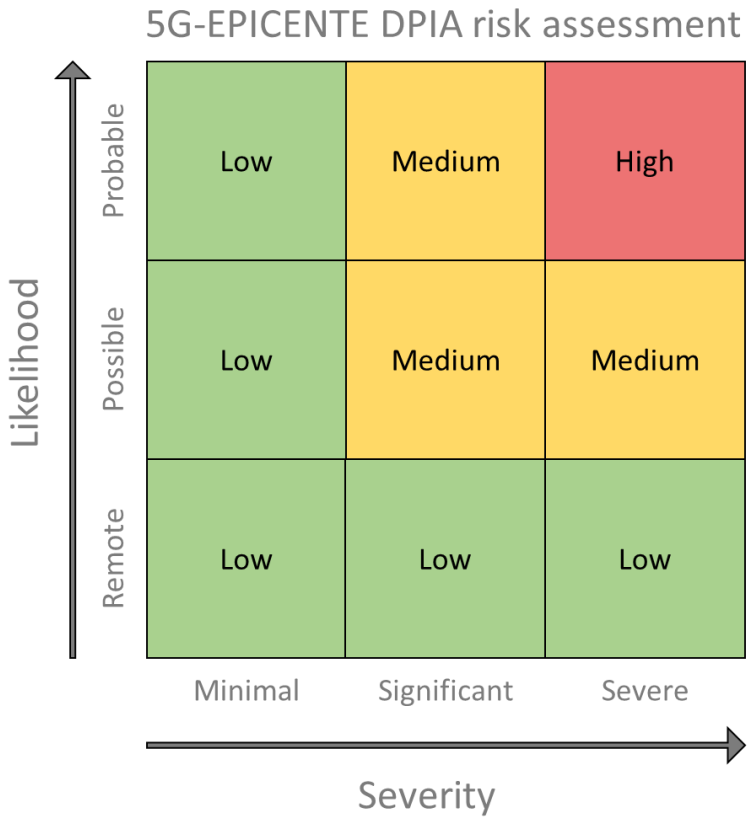


Figure 1: Risk assessment matrix for DPIA

Table 9: DPIA – Ethical risk assessment and mitigation measures

| Identification and assessment of risks and proposed measures to reduce risk | | | | | | | |
|---|---|---|---|---|---|---|---|
| **ER#** | **Describe source of risk and nature of potential impact on data subjects** | **Likelihood of harm** | **Severity of harm** | **Overall risk** | **Mitigation measures (to reduce or eliminate risk)** | **Effect on risk (eliminated, reduced, accepted)** | **Residual risk (Low, medium, high)** |
| ER1 | Data breaches may expose Hackathon participants identification and contact information, which may be used for spam and/or phishing attacks. | Possible | Significant | Medium | Anonymisation/ or, where it is not possible, pseudonymisation of personal data occurs by the data controller. | Reduced | Low |
| ER2 | Hackathon participants' personal information may be deleted from the database. In such case, it will not be possible to contact them. | Possible | Minimal | Low | Creation of backups of the data intended to be used for research purposes | Reduced | Low |
| ER3 | Hackathon participants' personal information may be altered in the database. In such case, contacting | Possible | Minimal | Low | Creation of backups of the data intended to be used for research purposes | Reduced | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | the affected participants may be compromised. | | | | | | |
| ER4 | Biometric and personal data collected during Use Case testing may be extracted and used for other purposes other than the ones defined in the project. | Possible | Severe | Medium | Biometric data are not linked to any personal data. Complete anonymisation before processing any biometric data | Eliminated | NA |
| ER5 | Biometric and personal data collected during Use Case testing may be deleted. | Possible | Minimal | Low | Creation of backups of the data intended to be used for research purposes | Reduced | Low |
| ER6 | Biometric and personal data collected during Use Case testing may be altered. | Possible | Minimal | Low | Creation of backups of the data intended to be used for research purposes | Reduced | Low |
| ER7 | Hacking of the Portal server to gain access to account data (*e.g.*, e-mail, passwords) | Probable | Significant | Medium | Data will be stored on a private server, accessible only through the internal network of the infrastructure. | Reduced | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ER8 | Unauthorised sign-in on the platform used for UC7 | Possible | Significant | Medium | Two-factor authentication required for successful connection to the GPS data platform | Eliminated | NA |
| ER9 | Leak of personal data (Email, Name, Surname, Country of Origin) collected for UC8 | Remote | Minimal | Low | Azure Cloud Security Measures, NDA on members that have access | Eliminated | NA |
| ER10 | Access of third-party developers to the platform from countries not participating in Horizon program or outside EU | Probable | Significant | Medium | A form will be available in the portal, where the location of the third-party experimenters shall be validated (via company details). | Reduced | Low |
| ER11 | Misuse of the platform by third-parties and/or not for its intended purpose (*e.g.*, testing of PPDR services) | Probable | Significant | Medium | During the lifetime of the project, access to third parties will be granted by the partners upon review. Moreover, access can be restricted by the testbed owners, who have control over their resources. | Reduced | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ER12 | Collection of critical information, such as partners' personal details in combination with bank details by ADS | Probable | Significant | Medium | All bank details are not linked to individuals but to entities. Only professional emails and phone numbers are stored in the Confluence pages, which are password protected. | Eliminated | NA |

# 5 Conclusions

In this deliverable, the legal and ethical framework, including relevant regulations and directives of the EC, has been presented. Specifically, the GDPR, the ePD, and the Free-Flow of Non-Personal Data Regulation have been analysed with respect to the activities foreseen in 5G-EPICENTRE.

Based on the input provided in the questionnaires circulated in the context of conducting a DPIA by the partners involved in data processing activities; and the discussions that have occurred during technical, non-technical and EB meetings, this deliverable has provided a set of actions, such as the use of informed consent forms in advance of processing any data. A clarification as to the criteria involved in recruiting research participants for the various project activities is also included. Moreover, based on the feedback obtained through the DPIA, the EB has created a list of ethical risks and their mitigation measures.

This deliverable constitutes the preliminary version of the DPIA, which will be further enriched, if needed, as the project progresses and its final version will be reported in D7.6, which is due in M36.

# References


[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, OJ L 119, 4.5.2016, p. 1–88.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995., p. 31-50.

[3] *Data subject rights and personal INFORMATION: Data subject rights under the GDPR*. (2021, August 21). I-scoop. https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/

[4] *Data Protection Impact Assessments*. Dataprotection.ie. https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments#:~:text=Under%20the%20GDPR%2C%20a%20DPIA,processing%20technology%20is%20being%20introduced.

[5] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance). OJ L 337, 18.12.2009. p. 11-36.

[6] European Commission. (n.d.). *Proposal for an ePrivacy Regulation*. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

[7] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) PE/53/2018/REV/1, OJ L 303, 28.11.2018, p. 59–68.

[8] Charter of Fundamental Rights of the European Union, 26 October 2012, OJ C 326, p. 391-407.

[9] *What are the GDPR consent requirements?* (2019, February 13). GDPR.eu. https://gdpr.eu/gdpr-consent-requirements/

[10] Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001: 2005. *ISO Management Systems*, *6*(1), 15-18.

[11] Information Commissioner's Office. (n.d.). *Sample DPIA template*. https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

# Annex I: Informed consent form template

**Informed Consent Form**

By signing the attached consent form, I understand that I agree to participate in the 5G-EPICENTRE project funded by the European Union (Grant Agreement no.101016521) and co-ordinated by AIRBUS DS SLC (ADS).

| | |
|---|---|
| I, the undersigned …… (name/surname) hereby declare that I agree to participate in this study, in the context of the 5G-EPICENTRE project | ☐ Yes<br>☐ No |
| I agree to participate in this activity in the context of the 5G-EPI-CENTRE project on the …… (date). | ☒ workshop/ questionnaire/ survey<br>*(*choose the appropriate field)* |
| The purpose of the study, the respective activities and my rights have been explained to me in writing (in the information sheet). | ☐ Yes<br>☐ No |
| I am participating voluntarily and understand that I can withdraw from the research activities without repercussions, at any time by the end of the study, and ask for my data to be deleted. | ☐ Yes<br>☐ No |
| I am satisfied that the assurances of responsible and strict data governance, given by the 5G-EPICENTRE project, will be upheld. | ☐ Yes<br>☐ No |
| I understand that my personal data are kept and treated as confi-dential as far as this research program is concerned. | ☐ Yes<br>☐ No |
| I know and understand that my personal data will be kept in a se-cure environment and that the data controller, as well as any data processors, will take all the necessary and appropriate measures to ensure the security, and in particular the confidenti-ality and integrity, of personal data, according to data protection legislation and the relevant guidelines. | ☐ Yes<br>☐ No |
| I explicitly declare that I agree with the publication of the results of this study in anonymous form and with the publication of se-lected screenshots for the promotion of the study in mass media, and / or scientific publications aimed at informing the public and / or the scientific community. | ☐ Yes<br>☐ No |

You may withdraw your consent at any time by submitting a request in writing to this address: *(email address of the organizer, Name of the organizer)*

Print name (participant) …… Print name (organizer) ……

| Signature (participant) | Signature (organizer) |
| --- | --- |
| …… | …… |
| Date | Date |
| …… | …… |