5G experimentation environment for 3rd party media services

D7.8 Report on legal ethics and gender monitoring- Intermediate

Document Summary Information

Grant Agreement No	101016714	**Acronym**	5GMediaHUB
Full Title	5G experimentation environment for 3rd party media services		
Start Date	01/01/2021	**Duration**	36 months
Project URL	www.5gmediahub.eu		
Deliverable No/Title	D7.8– Report on legal ethics and gender balance monitoring - Intermediate		
Related Work Package	WP7	**Related Task**	Task 7.4
Contractual due date	30/03/2021	**Actual submission date**	26/03/2021
Type	Report	**Dissemination Level**	Public
Deliverable Editor	Barbara Ferraioli (PIIU)		
Contributors	Maurizio Cecchi (PIIU)		
Peer Reviewers	Ronan Frizzel (ILS) and Sarang Kahvazadeh (CTTC)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101016714

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V1.0	15/01/2021	10%	Initial Deliverable Structure	Barbara Ferraioli (PIIU)
V2.0	31/01/2021	10%	Quality Review	Maurizio Cecchi (PIIU)
V3.0-7.0	23/02/2021	90%	Intermediate Versions with Updated Content	Barbara Ferraioli (PIIU)
V8.0	01/03/2021	95%	Version ready for Peer Review	Maurizio Cecchi (PIIU)
V9.0	07/03/2021	95%	Peer review and Quality Check	Ronan Frizzel (ILS) and Sarang Kahvazadeh (CTTC)
V10.0	10/03/2021	96%	Document ready for final check	Barbara Ferraioli (PIIU)
V11.0	17/03/2021	98%	QA Review	Vasilis Machamint (EBOS)
Final	24/03/2021	100%	Final version for submission	Barbara Ferraioli (PIIU)

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
5G-PPP	5G Infrastructure Public Private Partnership
ALLEA	All European Academies
CA	Consortium Agreement
DoA	Description of Actions
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
eMBB	enhanced Mobile BroadBand
EAB	External Advisory Board
EC	European Commission
ENISA	European Union Agency for Cybersecurity
EPCIS	Electronic Product Code Information Services
ESF	European Science Foundation
EU	European Union
FRA	Agency for Fundamental Rights
GA	Grant Agreement
GDPR	General Data Protection Regulation
GS	Global Standard
GUI	Graphical User Interface
IDE	Integrated Development Environment
IDEF	Integrated Definition Methods
IoT	Internet of Things
IPSE	IoT Privacy, Security and Safety Supervision Engine

KPI	Key Performance Indicator
KOM	Kick Off Meeting
LL	Living Lab
mMTC	massive Machine Type Communication
IDN	Interactive Digital Narrative
MS	Milestone
MCDN	Multi Content delivery Network
NDA	Non-Disclosure Agreement
NIS	Network and Information Security Directive
OB	Outside Broadcasting
PM	Project Meeting
PoC	Proof of Concept
PPP	Public Private Partnership
PR	Peer Review
QoE	Quality of Experience
QA	Quality Assurance
QM	Quality Manager
RE	Risk Exposure
RI	Risk Impact
RM	Review Meeting
RTD	Research and Technical Development
SCM	Source Code Management
TM	Technical Meeting
UGC	User Generated Content

UHD	Ultra High Definition
UML	Unified Modelling Language
URLLC	Ultra-Reliable Low-Latency Communication
VCDN	Virtual Content Delivery Networks
VR	Virtual Reality

Executive Summary

This document is identified as D7.8 and entitled “Report on legal, ethics and gender monitoring - Intermediate” is the result of activities performed in WP7 and WP8. The document has been merged with D8.1 “H-requirement no.1”.

This document provides the reader with an initial report on 5GMediaHUB project activities around legal and ethics and its implementation in technical work, including the Research Ethics Protocol.

In this document we will set the principles to investigate, design and monitor the procedures and protocols necessary for handling legal issues during the project’s lifetime. It will also set out the ethics requirements that the project must comply with (e.g., procedures, criteria to identify/recruit research participants, templates for informed consent, etc.) and manage the ethical issues concerning the design of the information and consent forms that will be used in case of involvement of humans through use case validations, whilst ensuring adherence to GDPR and the Policy, as outlined in this document. Preparation of the ethical, legal guidelines and the research ethical protocol is part of deliverable D7.8 stipulating the ethical principles that the 5GMediaHUB partners will adhere to in their work. Gender balance will also be monitored during the course of the project to ensure that the female/male ratio is maintained as close to 1:1 as possible for people employed during its course (Output: D7.8, D7.9, D8.1).

The consortium is fully committed to adhere to the highest ethical, fundamental rights and legal standards, as recognised at the European Union and International levels, including *the Charter of Fundamental Rights of the EU (2000/c 364/01), the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)* and *the European Code of Conduct for Research Integrity.* The research will be conducted basing on the following ethical ground rules:

- ***Reliability*** *in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.*
- ***Honesty*** *in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.*
- ***Respect for colleagues****, research participants, society, ecosystems, cultural heritage and the environment.*
- ***Accountability*** *for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.*

This first version (D7.8) is a set of legal and ethics guidelines to drive the 5GMediaHUB partners in their research activity. Its main aim is to create awareness about ethics and legal issues inside the consortium and to create a mindset shared among partners to prevent potential risks by applying a set of common methods and procedures for the project research process.

1 Introduction

1.1 5GMediaHUB approach to ethics, legal and gender issues

The 5GMediaHUB project will build and operate an elastic, secure and trusted multi-tenant service execution environment based on an open cloud-based architecture and APIs, by developing and integrating a testing and validation system with existing 5G experimental testbeds, for enabling the fast prototyping, testing and validation of novel 5G services and applications for the media vertical, thus reducing the entry barrier to 3rd party application developers. It aims at offering a DevOps environment for 3rd party media applications developers and experimenters, which will hide the complexity of service deployment, and deliver a 5G testing playground for media applications. Furthermore, leveraging the NFV Infrastructures of its 5G-PPP testbeds in Oslo (i.e., TNOR's 5G-VINNI) and in Spain (i.e. CTTC's 5G testbed in Barcelona), 5GMediaHUB will offer "Platform as a Service" (PaaS) capabilities via a set of open-standards Northbound APIs. These APIs will automate service management and resource allocation under varying load conditions and guarantee secure tenant isolation. Finally, 5GMediaHUB will offer a service catalogue of NetApps that offer common PaaS functionalities for the media industry, a Media Server, virtual Content Delivery Networks (vCDN), as well as many out-of-the-box security functions. In addition, 5GMediaHUB's aim is to deliver an adaptive, application-aware NFVI that optimally serves the media industry, by promoting rapid prototyping, optimising Quality of Experience (QoE), and leveraging standardised solutions and interfaces that promote interoperability with other application domains. To realise the above, the 5GMediaHUB consortium will encourage 3rd party media application developers, such as innovative SMEs, media content and service providers, and NetApps developers, who may not have access to 5G testbed infrastructures, the opportunity to experiment, test and validate their media and entertainment applications under realistic conditions thus significantly reducing any uncertainties before actual commercial service deployment.

The consortium is fully committed to adhere to the highest ethical, fundamental rights and legal standards, as recognised at the European Union and International levels, including the Charter of Fundamental Rights of the EU (2000/c 364/01), the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the European Code of Conduct for Research Integrity. The research will be conducted based on the following ethical ground rules:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.
- Respect for colleagues, research participants, society, ecosystems, cultural heritage and the environment.
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.

In addition, concerning risk management and legal compliance, all participants to the project will be made aware of their obligations as potential data processers (where appropriate) as well as issues beyond data and information protection and privacy described above. Actions will be taken to ensure that those handling subjects identifiable or sensitive information are made fully aware of their responsibilities and obligations to respect confidentiality in compliance with market standards (e.g.: ISO/IEC 27001:2005), best practices and legal requirements under the GDPR, as detailed in the Data Management Plan. In addition to the more general and EU wide guidelines, partners will adhere to and respect national regulations and laws. All partners are aware of their responsibilities in that sense and will follow the established rules.

1.2 Mapping 5GMediaHUB Outputs

Purpose of this section is to map 5GMediaHUB's Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to 5GMediaHUB's GA Deliverable & Tasks Descriptions

GA Component Title	GA Component Outline	Respective Document Chapter(s)	Justification
TASKS			
Task T7.4 Legal, ethics, gender balance (Leader: PIIU)	This task will investigate, design and monitor the procedures and protocols necessary for handling legal issues during the project's lifetime. It will also set out the ethics requirements that the project must comply with (e.g. procedures, criteria to identify/recruit research participants, templates for informed consent, etc.) and manage the ethical issues concerning with the design of the information and consent forms that will be used in case of involvement of humans through use case validations, whilst ensuring GDPR and Privacy Compliance Policy. Preparation of the ethical, legal guidelines and the research ethical protocol as part of deliverable D7.8, stipulating the ethical principles that the 5GMediaHUB partners will adhere to in their work.	The structure of this document respects the logical flow of the activities carried out on Task7.4. After a brief introduction outlining the objectives of this deliverable chapter 2 "European Legal framework" provides reader with an introductory paragraph on the EU definitions of research ethics on human beings' involvement. Chapter 3 "5GMediaHUB procedures and Guidelines" describes Procedures and guidelines. Chapter 4 "Ethics Protocols", is based on identified legal and ethics 5GMediaHUB	Chapter 2 lists the international ethics standards, legislations and codes used by 5GMediaHUB to lay the foundation of legal and ethics 5GMediaHUB background framework. Chapter 3 analyses the inclusion of individuals in project activities as well as use cases/scenarios, as described in D1.1, in order to identify potential ethics concerns. Chapter 4 described the background framework and the ethics concerns, describes criteria and procedures to be adopted by the partners during the whole lifecycle of the project.
DELIVERABLE			
D7.8 Report on legal ethics and gender monitoring - Intermediate			

1.3 Deliverable Overview and Report Structure

The structure of this document respects the logical flow of the activities carried out on Task7.4, i.e.:

- After a brief introduction outlining the objectives of this deliverable D7.8 and D8.1, chapter 2 "European Legal Framework" provides reader with an introductory paragraph on the EU definitions of research ethics on human beings' involvement. This chapter lists the international ethics standards, legislations

and codes used by 5GMediaHUB to lay the foundation of legal and ethics 5GMediaHUB background framework;

- Chapter 3 "5GMediaHUB Procedures and guidelines" analyses the inclusion of individuals in project activities as well as use cases/scenarios, as described in D1.1, in order to identify potential ethics concerns;
- Chapter 4 "Ethics Protocols", based on identified legal and ethics 5GMediaHUB background framework and the ethics concerns, describes criteria and procedures to be adopted by the partners during the whole lifecycle of the project.

Figure 1 shows the schema for defining the Research Ethics Protocol, and consequently provides the reader with an overview of the logical flow of the activities carried out in Task 7.4

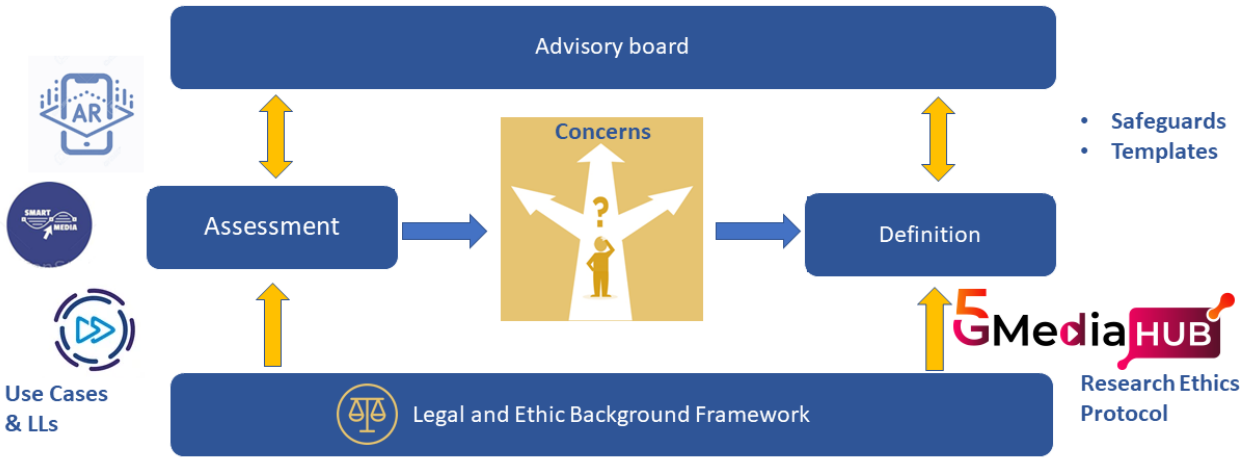

Figure 1:Ethics Protocol

1.4 Mapping of ethics, legal and gender issues in 5GMediaHUB

Purpose of this section is to map 5GMediaHUB Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

In all cases, 5GMediaHUB will thus adopt some safeguards, while the proper monitoring of these aspects will be executed by the Project Coordinator, the Technical Manager and the Ethics Manager/Data Protection Officer. Specifically, 5GMediaHUB will carefully take into account legal and ethical issues in relation to the project methodology, objectives and impact, and specifically T7.4 about Legal framework, ethics & gender balance which identify research ethics and data protection requirements respectively. Moreover, early in the project, interested partners will be required to appoint their own Data Protection Officers and to provide the project with a statement declaring that they will follow national and EU legislation during trials, including the compliance with the General Data Protection Regulation.

The interested 5GMediaHUB partner will remain responsible for any personal data collected during its own research. The interested partner will also be required to provide evidence of the authorisation to collect personal data, before access to or use of such data be granted. If defined by the European and national legislative framework, such authorisations will need to be requested by the specific partner to the appropriate competent authority in the partners' countries or, alternatively, to their own internal Ethical Committee.

In addition, appropriate procedures and state-of-the-art technologies will be applied for data collection, storage, protection, retention, destruction, and confirmation. A Data Management Plan detailing all those procedures for project data will be provided by the deadlines agreed in Task 5.2 (deliverables D5.3, D5.4).

2 European legal framework

Legal and ethics research conduct implies the application of fundamental legal and ethics principles to scientific research. The main ethics foundation of the 5GMediaHUB project consists of ***ensuring respect for people and for human dignity and fair distribution of the benefits and burden of research, and that we will protect the values, rights and interests of the participants.***

The following list identifies the main references to international ethics standards, legislations and codes regarding the legal and ethics concerns and that lay the foundation for the 5GMediaHUB legal and ethics background frameworks:

- Charter of Fundamental Rights of the EU (2007/C 303/01 [1]), repealing older version 2000/C 364/01.
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 [2]), repealing Directive 95/46/EC.
- European Charter for Researchers (2000) [3].
- Ethics in Social Science and Humanities (European Commission, DG Research and Innovation) (2018) [4].
- Horizon 2020 Programme Guidance How to complete your ethics self-assessment (2019) [5].
- Guide for Research Ethics Committee Members (Steering Committee on Bioethics (2012) [6].
- Regulation on Privacy and Electronic Communications (ePrivacy Regulation, 2017 [7]), repealing Directive 2002/58/EC.
- Directive 2006/54/EC (2006) on the implementation of principle of equal opportunities and equal treatment of men and women in matters of employment and occupation [8].
- Handbook on European non-discrimination law. (2010) [9].
- Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted on 28 January 1997, as well as the modernised "Convention 108 +" (April 2019) [10].
- Copyright Directive (Directive EU 2019/790 [11]) of 17 April 2019 on copyright and related rights in the Digital Single Market, amending Directives 96/9/EC and 2001/29/EC.
- Directive on security of network and information systems (NIS Directive) (Directive (EU) 2016/1148 [12]) concerning measures for a high common level of security of network and information systems across the Union.
- Cybersecurity Act (Regulation (EU) 2019/881 [13]) of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, repealing Regulation (EU) No 526/2013.
- Rome Declaration on Responsible Research and Innovation in Europe, 21 November 2014 [14].

Moreover, the consortium commits to upholding the highest ethics standards for research, as delineated in the **European Code of Conduct for Research Integrity** of All European Academies (ALLEA) [15], that was originally published in 2011 jointly with the European Science Foundation (ESF), which states specifically:

Researchers, academies, learned societies, funding agencies, public and private research performing organisations, publishers and other relevant bodies each have specific responsibilities to observe and promote good research practices and the principles that underpin them. Good research practices are based on fundamental principles of research integrity. They guide researchers in their work as well as in their engagement with the practical, ethical and intellectual challenges inherent in research. These principles are: Reliability, Honesty, Respect, Accountability.

3 5GMediaHUB Procedures and Guidelines

3.1 Purpose

According to the DoA, 5GMediaHUB is a 5G-PPP project supporting the EC's 5G policy by implementing the last phase of the 5G-PPP roadmap. It aims to prove and validate that 5G provides prominent industry verticals with ubiquitous access to a wide range of forward-looking services with orders of magnitude of improvement over 4G, thus bringing the 5G vision closer to realisation.

This will be achieved through conducting advanced field-trials of innovative use cases, **directly involving end-users** across five significant industry vertical domains.

In particular, 5GMediaHUB will provide:

- Validation of innovative and heterogeneous use cases that require 5G performance capabilities and that are expected to have a high future commercialisation potential. These use cases will be field trialled separately as well as concurrently with real end-user actors, thus validating their conformance to target 5G KPIs specified for each use case, as well as their business potential, ethics and social acceptance.
- Technological enablers for facilitating the execution of the field trials in an automated way, including (i) a unified cross-domain service orchestrator enabling multi-domain slicing and 5G service lifecycle automation, (ii) an innovative smart KPI visualisation system for facilitating the near real-time analysis, presentation, benchmarking and performance validation of reference 5G network KPIs against pre-defined target values, (iii) intent-based APIs for stimulating innovation and fostering the development, portability and provisioning of new innovative applications by SMEs.

The 5GMediaHUB technical approach is based on a modular architecture in which the various NetApps are integrated together via open interfaces and APIs. These enablers will facilitate the measurement and visualisation of 5G KPIs of the vertical use cases in near real-time whilst exercised in the field, as well as benchmarking and access from multiple locations, whilst promoting openness for 3rd party developers for the development of new innovative applications.

The KPI visualization system is going to be designed utilizing a 3-tier architecture composed of the presentation layer, the business logic layer and the data access layer.

All the above provide the necessary flexibility for the system to adapt to new interfaces, data sources, GDPR compliant data processing, machine learning and representation requirements as may be required during the interfacing with the users.

In order to achieve the GDPR compliance, one of the main components of the KPI visualization system is the "Pseudo-anonymization: data anonymization based on GDPR compliance".

The following paragraph provides further details about the research process and methods conducted on 5GMediaHUB, based on work-in-progress deliverables D1.1, as well as the project DoA.

3.2 Internal Procedures

5GMediaHUB will involve individuals for the purpose of accomplishing its objectives and administering the Consortium Agreement. Therefore, individuals from project partners and their third parties will be involved in day-by-day activities as well as external experts and stakeholders taking part of project pilots.

All of them will be managed accordingly with the EU and national ethics laws and principles. In addition, the Consortium Agreement (CA) contains specific provisions about how personal data of individuals involved in the Project for the purpose of administering the CA or the GA will be processed and protected for the purpose of the project.

The following subsections identify which are the project activities that will foresee external (i.e., not belonging to project partners) individuals' involvement in order to identify potential ethics issues and related safeguards.

3.2.1 Advisory Boards

5GMediaHUB project management structure includes the support of an External Advisory Board (EAB), which composition has been established in the DoA.

The EAB comprises a well-balanced group of external "advisors" drawn from across Europe and embracing a range of knowledge of the project's focus areas the EAB will offer impartial external advice from technological, scientific, market, regulation, ethics, societal, economic and business points of view. The consortium seeks to validate its technology direction with the EAB.

3.2.2 Potential impact on legal and ethics aspects in 5GMediaHUB Use Cases

This section aims to present the 5GMediaHUB use case (UC) scenarios, as defined in the Grant Agreement to identify in bold potential impacts on legal and ethics aspects. The UC owners be advised of these potential issues and a specific process will be put in place to analyse if ethical issues do indeed exist in the areas highlighted: this process will mitigate any problems that might arise.

Scenario 1.1: Immersive 360o VR media experiences: Using specialised sensors at the VR headset, the video follows the user's head movement to present in real-time a 360º stereoscopic view at the headsets' UHD screens. This use case, which allows real-time 3D holograms of persons, captured over a green screen, to be inserted in a VR environment. The environment is also rendered in real time to provide adequate CPU resources to the InfinitySet engine as the workload increases.

The specific scenario to be tested in this use case will be to insert remotely-located teachers into a VR classroom environment to explain a concept to the users, that will feel presence as if they are the students. Although this compelling application is feasible today with wired connectivity to the InfinitySet engine, this use-case will leverage 5G technologies to facilitate untethered operation, which will significantly improve impressiveness and facilitate an unobtrusive 360º view. This will be handled via the ImmersiveMedia NetApp within an eMBB slice, which will greatly simplify the implementation of 360º VR applications, as it will handle the mapping of the 360º VR sphere to the current users' field of view.

Scenario 1.2: Interactive consumption of 8k and VR media content: This scenario will explore the future of media consumption, which involves UHD 8k and 360º VR media content streamed over 5G, and offering collaborative, interactive experiences. This use case scenario will facilitate the engagement with what is happening on the first screen via Second Screen technology, allowing users to interact on virtual spaces (e.g., social media), participate in polls and contests, and access additional content (e.g., character origins, actor interviews, etc.). Specifically, this use-case will leverage a new form of transmedia (i.e., multiscreen) storytelling, termed Interactive Digital Narratives (IDNs). For example, this material could include a 360º UHD video stream of an event (e.g., in a stadium or an opera), or other elements that are part of the storyline, such as a background radio transmission, a background or game object, etc., and will be initiated in specific storyline trigger points. Finally, this scenario will address synchronisation between the First and Second Screens, comparing the existing inline solution (i.e., inaudible cue marks embedded at the video content), with out-of-band synchronisation signalling to be implemented by the Streaming NetApp. This is expected to improve synchronisation, taking advantage of ultra-low latency and delay jitter connectivity of 5G networks.

Scenario 2.1: High quality UGC production services: This scenario involves testing a UGC media service scenario in the UGC production domain, highlighting the catalyst nature of 5G networks in advancing significantly the state of the art. It is expected that 5G will support the very high-density uplink transmissions from the same location, avoiding congestion and supporting NetApps workflows for such contents, all of which are not supported by existing 4G networks. When many people are at an event, e.g. in stadiums, then their UGC may provide additional "color" content from various angles and perspectives. Using it in professional video production poses further challenges, such as ensuring quality, reliability and authenticity. In addition, professional content encoding, transmission and synchronisation with external 4k video cameras must be ensured.

Scenario 2.2: Professional live production: Live productions are usually divided into indoors productions (i.e., in studios), or field productions (i.e. from the streets, sports venues, remote areas, etc.). The latter are expected to benefit the most from 5G, which brings significantly higher uplink capacities that will facilitate disruptive remote production pipelines. Thus, field production will not have to rely on Outside Broadcasting (OB) vans with on-site production teams, as UHD camera streams can be transmitted at the remote studio in real-time. This use-case will evaluate "edge-based field production" through the 5GMediaHUB Experimentation Facility to cover for the exponentially growing segment of outdoors production. The application to be demonstrated facilitates local sports events to be recorded and produced in real time.

Scenario 3.2: Smart city co-creation: This scenario demonstrates how visual media can be reliably distributed in multiple remote sites or domains, enabling interactive co-creation between citizens and the city. This scenario will be validated at both CTTC's and TNOR's 5G testbeds at the same time, and the Multi-Content Delivery Network (MCDN) NetApp will be leveraged for cross-domain media content distribution. The proposed idea relies on citizens (real users) being able to produce, share and distribute media assets on the go. 5G will facilitate sharing media assets in real time without bandwidth or user density limitations (e.g., for artistic events with a massive number of participants). During the use-case execution, multiple UGC streams will be concurrently streamed from TNOR's 5G testbed, and top ranked ones will be distributed across both facilities by the MCDN NetApp.

3.3 Main Legal and Ethics Concerns

The analysis carried out in this document is based on the information available at the current stage of the project (M3), when use cases details and the data management plan are still under discussion. It is thus not meant to be exhaustive, but to create the basis for an initial definition of the project Research Ethics Protocol that will be refined, if necessary, during the project lifetime.

Currently, some legal and ethics concerns are envisaged about:

- individuals' recruitment in the EAB and during the pilots;
- their personal data protection and
- confidentiality of project data communicated in particular to EAB members who will participate to the project meetings and review some project deliverables, as well as Living Lab participants when involving end-users external to the project.

4 5GMediaHUB Ethics Protocol

As a result of the analysis carried out in the previous section, this section will outline the guidelines for the 5GMediaHUB consortium on ethics. In particular, the following subsections will:

- Describe project ethics management safeguards (4.1);
- Define recommendations for the arrangements for recruitment (4.2), including the description of the criteria and the procedures for human beings' involvement in the project research activity;
- Define recommendations in order to protect individuals' data (4.3), including an overview of the EU framework on data protection and the project ethics rules;
- Define protocols in order to protect project data (4.4).

4.1 5GMediaHUB Safeguards

To assure compliance with ethics principles, 5GMediaHUB has established some safeguards:

- The current Research Ethics Protocol has been defined to guide project activities.
- A project Legal & Ethics Manager and the project DPO has been appointed respectively in the person of Barbara Ferraioli from PIIU (Legal & Ethics Manager).
- An Ethics Panel chaired by the Legal & Ethics Manager, that includes legal advisors of the participating members (experts on ethics, privacy and legal issues) is available for advices and will monitor project activities compliance with the current Research Ethics Protocol. At the time of writing the current document, the composition of the Ethics Panel is the following:
    - Barbara Ferraioli from PIIU, Legal & Ethics Manager and EP Chair
    - Pat O'Sullivan from Inlecom Group, as IPR expert
    - Christos Verikoukis from CTTC as project coordinator
- In case of any specific issue should arise, an external expert will be invited to the Ethics Panel, to act as independent reviewer and consultant.
- A Project Management Board (PMB) is constituted and is composed of different manager roles that ensure the quality conduct of research activities and the protection of the rights of participants.
- A specific report will update the progress (i.e., D7.9 - Report on legal and ethics monitoring, expected at M35).

4.2 Guidelines for external experts' involvement

Recruitment of external research participants will be governed by three key principles ([6]) that:

- The participation is *voluntary*;
- Recruitment is *appropriate to the research question and methods*; and
- Participants are *chosen in a non-discriminatory manner*.

4.2.1 Involvement Criteria

4.2.1.1 Participants Freedom

When performing research activities with humans, 5GMediaHUB will strictly observe the guidance and direction given in [1], [3] and [4]. For each investigation activity, details on the used procedures and criteria will be readily made available to the project external participants. It is at the participant's discretion as to whether s/he wishes to participate in the investigation activity or not.

4.2.1.2 Inclusion and Non-Discrimination

Concerning the inclusion of human beings in use cases, External Advisory Board and Living Labs activities, 5GMediaHUB will comply with relevant national and international regulations, and special attention will be paid to the observance of the DIRECTIVE 2006/54/EC [8] of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), Article 14 of and Protocol 12 to the European Convention on Human Rights, as well as the Handbook on European non-discrimination law [9] issued by the EU Agency for Fundamental Rights (FRA) – 2018 edition.

4.2.1.3 Research Integrity

Good research practices are based on research integrity. Ensuring a good research environment means increasing trust in researchers who will be better engaged with the practical, ethics and intellectual challenges inherent in their research. Thus, the key principles of research integrity will be the final recruitment criteria of 5GMediaHUB: “reliability”, “honesty”, “respect”, “accountability” (European Code of Conduct for Research Integrity [15]).

4.2.2 Involvement Procedures

As a general rule, the identification and selection of the research participants will be carried out by the pilots site leaders. They will recruit participants from among their networks, according to the profile determined for the purposes of testing the 5GMediaHUB tools. Participants will be invited to participate according to their role within the organisation that potentially can be relevant for the 5GMediaHUB project activities. The following more specific procedures will be adopted to respond to determined risks and obstacles:

4.2.2.1 Rights of Participants

Complying with the *European Charter for Researchers*, 5GMediaHUB has considerable responsibility for the people involved in the research action and for their rights, safety, well-being and interests or dignity, integrity, rights, and autonomy. This approach applies to all the communities that are engaged and involved in the research, or, in other words, for the “society at large, also in terms of avoiding potential misuse or unintended consequences of research results.” [3]. Therefore, participation in 5GMediaHUB project activities will be fully voluntary and all participants will be given the opportunity to ask questions and receive understandable answers before making decisions about their participation. Participants will also have the right to withdraw themselves and their personal data and terminate their participation in the research at any time and will be reminded about their rights before participation. Participants will be given this information via an information sheet as shown later.

4.2.2.2 No Discrimination

To avoid discriminatory outcomes before the research activities (i.e., during the selection process) and after (i.e., during the dissemination and exploitation phases), all the necessary measures will be enforced to safeguard against stigmatization of groups and individuals on account of their gender, race, religion, sexual orientation, political beliefs, ethnicity, and other social features.

5GMediaHUB will make best efforts to recruit women (female/male ratio will be maintained as close to 1:1 as possible) and persons of diverse backgrounds through processes that are inclusive, clear, accessible, and transparent. Any exclusionary practices, marginalization, devaluation of research, and stereotyping will be considered unacceptable.

4.2.2.3 Fairness of Process

In order to ensure that information is properly and effectively understood by the participants, for each project activity involving human beings, 5GMediaHUB team will:

- Provide tailored protocols with details on procedures. Moreover, the chosen criteria to be used will be readily made available to the participants.
- Ensure that potential participants will be fully informed and will not feel pressured or coerced into giving consent, to this aim, in fact, different procedures will be deployed. This ensures the respect of freedom of the participants as requested by reference [2];
- Provide any information (being it written or recorded) in a language and in terms the participant can fully understand. This ensures the unambiguity and avoids misunderstanding and incomprehension, as required by reference [2];
- Explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw his/her participation, samples or data at any time, without any consequences. This ensures the respect of freedom of participants to contribute or not;
- Describe the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomfort that might ensue. This ensures the right of participant to be informed about any consequences (also potential risks);
- State which procedures will be implemented in the event of unexpected or incidental findings (in particular, whether the participants have the right to know or not about any such findings);
- Provide researchers contact details for participants to contact the Project Consortium for information and decide whether they wish to join in.

4.2.2.4 Ethics Practices

To guarantee the respect of the principles of the research integrity, specific research practices will be adopted to:

- Enhance the research environment.
- Stimulate training, supervision and mentoring.
- Promote open, transparent and non-discriminatory research procedures.
- Incentive collaborative working.
- Give results of publication and dissemination avoiding research misconducts such as: falsification and image manipulation; plagiarism; duplicate and redundant publication.

4.3 Gender aspects, sex & gender analysis

The 5GMediaHUB consortium is convinced that, in agreement with the Vade Mecum on Gender Equality in Horizon 2020, an '*in-depth understanding of men and women's needs, behaviours and attitudes can improve the scientific quality and societal relevance of the produced knowledge, technology and innovation*'. We recognise that the end-users of the media applications have different characteristics (gender identities, sex, age, ethnicity, profession, occupation, education, income, age, interests, household and living arrangements, familiarity with and attitudes towards technology, etc.). In addition, we are aware of the role that gender can play with regards to the technologies to be developed. We will systematically analyse the relevance of sex/gender when it comes to the different expectations males and females may have towards 5GMediaHUB innovation. This approach is formally included in the Grant Agreement and in the Description of Work.

Our innovation and the project will consider the gender dimension and cater for the needs, motivations and differences between the requirements analysis in WP1: A balanced participation of male and female professionals will allow gender analyses to be incorporated into the early user requirement definition. We will sex-disaggregate the data, as per the recommendations of the EIGE, to find out whether different expectations regarding the GUI interfaces, features, functionality, etc., exist based on sex/gender.

- Throughout the development of the Experimentation Tools components in WP2: The GUI interface design of the Experimenters Portal will be consulted with both males and females at different ages, and posterior alpha and beta versions will be trialled by both males and females. We will pay attention to

gender differences of perception, understanding, cognition and reaction when it comes to the development of the system.

- During the validations and the evaluation of results in WP4: In terms of usage, the innovation will benefit both males and females equally, either as direct or indirect end-users. During the validation of the Experimentation Facility and the NetApps through the use cases, we will also consider particularities of behaviour, and ensure diversity and gender balance within test groups.

In our exploitation, dissemination and communication activities in WP5 and WP6: We will consider gender in the training and education materials, in the target groups of the community building and outreach activities as well as in the business models. This is important in ensuring the education of the current professional and next generation of scientists and others needed in the EU to maximise its creativity and innovation potential.

4.4 Privacy as an overall rule

4.4.1 EU Framework on Data Protection Overview

The current EU framework on data protection, the General Data Protection Regulation [2], defines (article 4, n. (1)) the personal data as ***any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or will more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of That natural person***.

Therefore, the scope of personal data is broad, including anything that can uniquely identify an individual, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.

Moreover, Article 4 of the GDPR includes definitions of specific personal data, which are mostly related to sensitive and peculiar aspect of the personality of physical subjects, and notably:

- **Genetic data**: *personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question [article 4, n. (13)];*
- **Biometric data**: *personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data [article 4, n. (14)];*
- **Data concerning health**: *personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status [article 4, n. (15)].*

Furthermore, processing of personal data being able to reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are, in general, prohibited and may be processed exclusively in some specific cases. These categories of personal data that are subject to additional protections, as they are considered as the core of the protection that must be ensured to individuals by privacy regulations.

In the eventuality of personal data processing, the GDPR introduces a range of requirements, constraints and controls to govern how personal data should be collected, stored, processed, retained, and shared. The most significant are hereafter listed:

1. Individuals shall provide **explicit consent** to data collection – "consent by default" is not valid. The organization seeking consent shall also provide clear information on how that data will be used, for how long it will be retained, and how it will be shared with third parties. Individuals can retract consent at

any time, without prejudice. Additional permissions shall be requested from the individual if the data is to be used for processing purposes beyond the original consent.

2. A **Data Protection Officer** (DPO) shall be designated.
3. Organisations shall conduct a **Data Protection Impact Assessment** (DPIA) to understand personal data risk exposure.
4. If the processing would result in a high risk in the absence of measures taken by the organisation to mitigate the risk, the **supervisory authority prior to processing shall be consulted**.
5. Data protection shall be **by design and by default**, requiring data protection mechanisms to be embedded into products and services from the earliest stage of development, and the adoption of strictest privacy settings without any manual input from the end user.
6. **Individuals' rights** shall be guaranteed:
    - Individuals shall have easier access to their data, enabling them to review what data is stored about them and how it is processed, who it is shared with, along with the ability to migrate that data between service providers without restriction.
    - Individuals shall have the "right to be forgotten", also known as "right to erasure", so that there is no legitimate reason for an organization to refuse the request of individuals to definitely remove their personal data when they ask for it to no longer be retained.
7. **Profiling and automated decision making** shall ensure the profiling data subjects' rights.
8. Any **data breach** shall be notified to the Data Protection Authority.
9. Personal data processed for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes.

All those requirements are included in 5GMediaHUB Research Ethics Protocol and illustrated in the following sub-sections.

4.4.2 Personal data processing

The data collected in the project will be comprised of raw measurements and observations from testing and validation trials, logs exposing the state of the experiments, source code used to generate experiments, scripts used for the analysis of raw measurements and artifacts generated by them. Raw measurements, for e.g. network and service-level KPIs with related parameters, such as timestamps, etc., are stored in plain text format, such as comma separated values (CSV). The raw measurements will be pre-processed at the time of data-collection to remove any personally identifiable information, such as IP address, leaving only anonymous and unique machine identifiers along with other parameters related to computations.

The consortium has collectively affirmed that none of the data managed, shared, processed or analysed by the 5GMediaHUB system will pertain to personal data of any EU citizens, as the nature of the 5GMediaHUB data sets are highly network, test, protocol and instrumentation related. However, network measurement techniques, such as IPFIX and DPI might include some personal information, such as total network usage and specific applications used, which can be inferred through source IP and MAC addresses. While anonymising or masking such information will render it unsuitable for analysis tools and algorithms, pseudonymisation will be used, based on GDPR stipulations. With this technique, personal data is replaced with artificial identifiers, while remaining suitable for data analysis and also providing the ability to restore data to original state, crucial to identifying malign sources.

For what concerns data related to individuals participating in project workshops, events, interviews and trials, as a general rule, only **anonymised** or **aggregated data** (completely disjoined from people identification and profiles) will be processed. Organisational and technical mechanisms for the anonymisation and encryption of any personal data to be logged in the various systems at the trials site facilities will be adopted.

As stated in the previous subsection about involvement of human beings in the research, specific Information Sheets and Informed Consent Forms will be provided to participants. Collected data will be definitely removed

after the execution of the testing and validation phase. **The 5GMediaHUB Draft Information sheet** and **Informed consent form** are provided in chapter 4.5.1.

4.5 Data protection and Information Security

5GMediaHUB will not involve:

- Activities or results raising security issues;
- 'EU-classified information' as background or results.

This initial assessment does not preclude a different assessment following the security scrutiny. Should the members of the Information and Communication Technologies Programme Committee consider that 5GMediaHUB involves security-related activities or produces outputs that need to be classified, special provisions for classified information (as defined in the Commission Rules of Procedure (Decision 2015/444/EC, ECSC, Euratom, and further explained in the Guidelines for the classification of research results) will be taken in the grant agreement, as necessary and appropriate.

As general rule, only **anonymised or aggregated da**ta (completely disjoined from people identification and profiles) shall be processed related to the participation in the project research process and data generated or processed by the project (e.g., during the pilots).

Whenever for specific reasons personal data might need to be processed, the interested 5GMediaHUB partner shall remain responsible for the data collected during its own research and will be required to follow the European and national rules on privacy and data protection as well as the hereafter ethics rules.

4.5.1 Consent Procedures

As abovementioned, explicit consents to personal data collection have to be provided by each interested individual, prior to their involvement in the project activities.

The GDPR [2] defines consent of the data subject as *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*.

As well as the Recital 32 "Conditions for Consent" in [2] declares that consent shall be given by a clear affirmative act establishing a **freely given, specific, informed and unambiguous** indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

Consent is not just a simple form or document to be filled and signed by the individual, but above all a process that involves the individual and the entity entitled to collect and manage data.

The most important aspect in the process of an informed consent is to **unambiguously** ensure that individual is properly informed in a comprehensive language and that individual effectively **understands** the research activity, how data are used and the risks to be harmed (if any).

In this perspective, the process of informing project activities participants and ensuring their understanding shall be carried out by considering the following conditions in order to:

- Ensure the specificity of consent, an ad-hoc tailored consent form shall be distributed to all individuals, prior their involvement in project activities that collect personal data. In case of processing of "special category of personal data", those participating will have a separate consent form, with a paragraph adding more details on the purpose of the processing, the duration of the processing, the plans for storing and sharing that data and their rights of access, correction and erasure. This data will be destroyed as soon as possible after the specific objectives to which the data relates are achieved;
- Reduce the risk of ambiguity, misunderstanding and incomprehension, the consent form to be filled and signed shall be translated into participant's mother tongue;

- Reduce the risk of access to the information, the consent form shall be provided to participants either in hard copy or online;
- Be compliant with the "Privacy by Default" principle, as well as to respect the freedom of individuals, consent form shall not provide "default checked answers" that can dissuade to express particular opinions and trigger to "pure acceptance" behaviour of participants;
- Respect the freedom of the individuals, informing phase and understanding phase shall be carried out by ensuring necessary time to take the right decision and consequently sign or not the consent form.

As abovementioned, any consent form shall be produced and customised for each activity.

The informed consent is composed by two parts: the Information Sheet and the Consent Form. Both shall be distributed among participants prior the activity will start. The Informed Consent Form, duly signed by the individual or his/her legal representative, shall be kept secure and on file for the whole duration of the project by the activity organizer, who shall notify it to the Ethics Panel using the relative email address.

Consequently, a template to be customised on the specific project activity is included here:

5GMediaHUB for European Citizens

Information Sheet

5GMediaHUB is a 36-month EU-funded project with the purpose of conducting advanced field trials of innovative and thematically diverse digital services that require 5G capabilities and performance in the media sector directly engaging with end-user actors, so as to validate the technological performance of 5G technology in successfully serving them, as well as validate the business models and potential of these use cases prior to commercial deployment.

You are invited to join the **5GMediaHUB** research project to take part of the **5GMediaHUB** field study. Please take whatever time you need to read and understand the following text. The decision to join, or not to join, is up to you. if you agree with the content sign the consent form hereafter.

The aim of this activity is to *[ADD HERE THE DESCRIPTION]*.

Your participation is **voluntary and free-of-charge** and it will take you *[ADD HERE THE TIMEFRAME]* minutes/hours. If you accept to participate, you will be asked to *[ADD HERE DETAILS]*.

No risks are foreseen for your participation to this activity. *[IN CASE OF FORESEEN RISKS, ADD HERE DETAILS].*

The project may stop the field study or take you out of the field study at any time they judge it is in your best interest. They may also remove you from the field study for various other reasons. They can do this without your consent. On the other hand, you are free to stop participating at any time without any obligation.

5GMediaHUB will collect information for the purposes of the **5GMediaHUB** project. Only information that is necessary to address the central purpose of the research will be recorded. Your personal data will not be transferred outside the **5GMediaHUB** Consortium and, in any case, they will not be transferred outside Europe. Your personal data will be securely stored and retained for the lifetime of the project and safely deleted afterwards. All collected information will be handled in accordance with the provisions of the "Charter of Fundamental Rights of the EU" (2007/C 303/01), "Convention 108 +" of the Council of Europe for the Protection of Individuals and "General Data Protection Regulation" (EU Regulation 2016/679).

More details about **5GMediaHUB** privacy policy can be found at the following link *[ADD HERE THE LINK TO THE 5GMediaHUB WEBSITE PAGE].*

If you have any questions about the field study or the project itself, any problems, unexpected physical or psychological discomforts, any injuries, or think that something unusual or unexpected is happening, you are free to contact Mr./Ms. *[ADD HERE THE CONTACT PERSON]* at *[ADD HERE THECONTACT DATA – EMAIL – PHONE NUMBER]*.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101016714

After reading the Information sheet and voluntary deciding to take part of the project activity, participants shall sign the following Informed Consent Form. Since the form contains personal data, it has to kept secure by the activity organiser.

5GMediaHUB for European Citizens

Informed Consent Form

I *[ADD HERE THE PERSON'S NAME and SURNAME]* agree to voluntary participate to the **5GMediaHUB** field study.

Yes ◯ No ◯

I have read the Information Sheet, and understand what the field study involves.

Yes ◯ No ◯

I understand that if I decide at any time that I no longer wish to take part in this field study, I can notify the researchers involved and withdraw immediately, without any obligation.

Yes ◯ No ◯

I have had the opportunity to have all my questions answered to my satisfaction. I've been informed of the data governance given by the **5GMediaHUB** project.

Yes ◯ No ◯

I voluntary consent with the processing of my personal data in accordance with the provisions of the "Charter of Fundamental Rights of the EU" (2007/C 303/01), "Convention 108 +" of the Council of Europe for the Protection of Individuals and "General Data Protection Regulation" (EU Regulation 2016/679).

Yes ◯ No ◯

A copy of the information sheet and this signed consent form will be given to the signee.

Date _____

Signature of Subject or Representative _____

This project has received funding from the European Union's Horizon 2020 research and innovat programme under the Grant Agreement No 101016714

4.5.2 Designation of the Partner DPO

In the eventuality of personal data processing, the partner shall notify it to the project Ethics Panel. Moreover, in compliance with the above-described rules, the partner involved in collecting and/or processing personal data shall nominate a DPO well before the collection/processing will take place and communicate it to the project Ethics Panel and the Project Management Board.

Under the General Data Protection Regulation (GDPR), ex Art. 37(1), a DPO must be designated for personal data processing in any case where:

1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
3. The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Art. 37(5) of the Regulation details what are the requirements and skills for the role:

The DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

In particular, the tasks expected by Art. 39 of the GDPR include:

1. Informing and advising the controller or the processor and their employees who carry out processing of their data protection obligations (Art. 39(a)).
2. Monitoring compliance with the EU and national data protection rules, including the assignment of responsibilities and awareness-raising and training of staff involved (Art. 39(b)).
3. Providing advice where requested as regards the data protection impact assessments (DPIAs) and monitoring compliance and performance (Art. 39(c)).
4. Cooperating with the supervisory authority (Art. 39(d)).

Acting as a contact point for the supervisory authority on issues relating to processing (Art. 39(e)).

4.5.3 Data Protection Impact Assessment

Taking into account article 35 of the GDPR, the partner shall evaluate if the personal data processing is likely to result in a high risk to the rights and freedoms of individuals, taking into account the nature, scope, context and purposes of the type of processing. In this case, the partner shall conduct a data protection impact assessment well before the collection/processing will take place and report its results to the project Ethics Panel to be included in deliverable D7.9-Report on legal and ethics monitoring.

The GDPR Article 35 states that a DPIA is necessary where an organisation, processes personal data in a way that is likely to result in a high risk to the rights and freedoms of an individual.

GDPR Article 35(3) states that DPIAs are mandatory in a number of processing scenarios where an organisation performs automated decision-making based on personal data profiling, large scale processing of special categories of data or systematic monitoring of publicly accessible areas on a large scale.

In particular, a DPIA is required where an organisation:

- Uses systematic and extensive profiling with significant effects; or
- Processes special category or criminal offence data on a large scale; or
- Systematically monitors publicly accessible places on a large scale.

4.5.4 Declaration on Compliance and/or Authorisation

In case of collecting and/or processing personal data, the partner shall check if a declaration on compliance and/or authorisation is required under national law for collecting and processing personal data.

If yes, copies of the declaration on compliance and/or authorisation shall be kept on file for the whole duration of the project, by the partner. If no, declaration on compliance or authorisation shall be required under the applicable national law, a statement from the designated Data Protection Officer that all personal data collection and processing will be carried out according to EU and national legislation shall be kept on file for the whole duration of the project, by the partner.

In both cases, the above documentation shall be submitted to the project Ethics Panel to be included in deliverable D7.9-Report on legal and ethics monitoring.

Both actions shall be carried out well before the collection/processing will take place.

4.5.5 Data Protection by Design and by Default

Partners are requested to adhere to what is defined in Art. 5 of the GDPR, so that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency'**)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation'**)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation'**)
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**')
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation'**)
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality'**).
- the controller shall be responsible for, and be able to demonstrate compliance with 'accountability'.

4.5.6 Individuals Rights

The GDPR is designed to provide EU citizens with more control over their own personal data. Therefore, appropriate **procedures and state-of-the-art technologies** shall be applied for data collection, storage, protection, retention, destruction, and confirmation. Details on those procedures are defined in the project Data management Plan (DMP, i.e., D5.3 (initial) and D5.4 (final) Data Management Plan and Report).

4.5.7 Automated Individual Decision-making including Profiling

As stated by Art. 22 of the GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal impacts concerning that person or correspondingly altogether affects the person in question.

Automated processing and profiling are authorised if the decision is:

- Necessary for entering into, or performance of, a contract between the data subject and a data controller;
- Authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- Based on the data subject's explicit consent.

In case of automated processing and profiling, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Decisions referred by art. 22(2) shall not be based on special categories of "special category of personal data" (art. 9(1)), unless the data subject has given explicit consent (art. 9(2)(a)) or it is necessary for reasons of substantial public interest (art. 9(2)(g)) and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

4.5.8 Data Breach

In case of data breach, the GDPR states that disclosure within 72 hours must be made to the local Data Protection Authority, enabling individuals to be informed and take appropriate remedial action, while in case of organisations' non-compliance with the GDPR provisions, substantial financial recourse will be made against them.

4.5.9 Data Retention Time

Personal data generated or managed by the project shall be destroyed as soon as possible after the specific objectives to which the data relates are achieved.

4.5.10 Data Protection strategy

The CA has already defined in Section 10 the rules for the non-disclosure of Confidential Information in the project, so *that all information in whatever form or mode of communication, which is disclosed by a Party (the "Disclosing Party") to any other Party (the "Recipient") in connection with the Action during its implementation and which has been explicitly marked as "confidential" or "secret" at the time of disclosure, or when disclosed orally has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within 30 calendar days from oral disclosure at the latest as Confidential Information by the Disclosing Party is "Confidential Information".*

4.5.11 External references

This document describes the work performed in T7.4 "Legal and Ethics" during the first 3 months of the project. This includes the identification of 15 main references (i.e., international ethics standards, legislations and codes regarding the legal and ethics concerns) that lay the foundation for the 5GMediaHUB legal and ethics background framework.

Most of these references are repealing already existing regulations and/or directives, as well as these coming into force during the project lifecycle (e.g., new EU Cybersecurity Act published on June 7th 2019 and come into force on June 27th 2019).

This demonstrates the relevance of the argument and how background framework is still evolving and requires to be continuously monitored for ensuring the compliance of project activities with respect to current EU legal framework and research ethics concerns.

In case of needs, the Research Ethics Protocol will be accordingly revised and enhanced with the objective of ensuring the observance and promotion of good research practices and the principles that underpin them.

The second version of this document (D7.9) will be delivered at month 36 (end of project) and will report on the monitoring activity and the refinement (if needed) of the Research Ethics Protocol.

This document provides the 5GMediaHUB consortium with templates for information sheet, consent form and non-disclosure agreement for External Advisory Board as well.

In Annexes I, II, II and IV we include the ethics and legal statements of the partners that officially published their policies.

5 Conclusions

The document is based on the initial assessment of potential legal and ethics concerns relating to the project's activities as known at the current project stage. Thus, for this assessment, this document takes into account the first outcomes (even if work is still in progress) of the project's activities, and specifically the definition and analysis of use cases, methodologies for the validation of the NetApps and Description of Actions (DoA).

Indeed, the current available information about the project's external participations, as well as use cases/scenarios and the methodologies for the validation enable the understanding of:

i. How and when research will involve human beings,
ii. Initial potential legal and ethics concerns on individuals' recruitment,
iii. Protection of personal data and
iv. Protection of project data as well.

Based on this information, the guidelines and recommendations (representing the corpus of the Research Ethics Protocol) are defined in order to ensure compliance with the current legal and ethics framework, as discussed above.

Throughout the project, the 5GMediaHUB partners will adhere to the Research Ethics Protocol in their work and its implementation will be monitored and refined including an update on the review procedures: the second version of this document (D7.9) will be delivered at month 35 and will report on the monitoring activity and the revision of the Research Ethics Protocol.

Based on this background framework and the description of use cases/scenarios (still under development during the editing of this document, however details have been gathered from D1.1 preliminary description), the document foresees the potential legal and ethics concerns (i.e., Industrial data confidentiality and personal data protection).

Further analysis of the 5GMediaHUB project process and methods envisages additional legal and ethics concerns (i.e., personal data protection and confidentiality of project information), and specifically these relate to External Advisory Board (EAB) involvement in the project (i.e., participation to meetings and revision of deliverables), as well as participants of Living Labs (in case of end-users external to the project consortium).

By adopting a "concerns and safeguards" approach to foresee and address ethics issues, the document proceeds in the definition of the code of conduct, the 5GMediaHUB Research Ethics Protocol, to be respected during the whole project lifecycle, including the definition of Ethics Panel and its role, individuals recruitment rules, safeguards for ensuring privacy and personal data protection (i.e. information sheets and consent procedures), as well as for ensuring project data confidentiality (i.e. non-disclosure agreements).

6 References

[1] European Parliament, Charter of Fundamental Rights of the EU. (2007) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12007P

[2] General Data Protection Regulation (GDPR). (2016) - https://gdpr.eu/

[3] European Commission, European Charter for Researchers. (2000) - https://euraxess.ec.europa.eu/jobs/charter/european-charter

[4] European Commission, Ethics in Social Science and Humanities. (2018). https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf

[5] European Commission, Guidance How to complete your ethics self-assessment. (2019) - http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

[6] Council of Europe - Steering Committee on Bioethics, Guide for Research Ethics Committee Members. (2012) - https://www.coe.int/t/dg3/healthbioethic/activities/02_biomedical_research_en/Guide/Guide_EN.pdf

[7] European Commission, ePrivacy Regulation. (2017) - https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1565770573013&uri=CELEX:52017PC0010

[8] European Parliament, Directive 2006/54/EC. (2006) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0054

[9] European Union Agency for Fundamental Right, Handbook on European non-discrimination law. (2018) - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-handbook-non-discrimination-law-2018_en.pdf

[10] Council of Europe, Convention 108 +. (2019) - https://www.coe.int/en/web/data-protection/convention108/modernised

[11] European Parliament, Copyright Directive (Directive EU 2019/790). (2019) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790

[12] European Parliament, Directive on security of network and information systems. (2016) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

[13] European Parliament, Regulation (EU) 2019/881 (Cybersecurity Act). (2019) - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

[14] Presidency of the Council of the European Union, Rome Declaration on Responsible Research and Innovation in Europe. (2014) - https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf

[15] ALLEA, European Code of Conduct for Research Integrity. (2017) - https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

Annex I - WATERFORD INSTITUTE OF TECHNOLOGY (WIT)

For Ethics issues relating to research WIT have a Research Ethics Committee that regularly meets to assess projects and research being carried out within the organisation (see https://www.wit.ie/research/for_postgrads/research_ethics).

Good ethical governance and review of research is a core value and priority at WIT. It is the responsibility of the Research Ethics Committee, which is a sub-committee of WIT's Academic Council, to scrutinise all research which involves humans and animals to ensure it is compliant with statutory requirements and is conducted to the highest ethical principles which emphasise the rights and welfare of subjects (both people and animals), treating all with dignity and ensuring that those who participate in research, whether subjects, researchers, other stakeholders and/or WIT are not put at risk. Please, see https://www.wit.ie/images/uploads/Policies_PDF/WIT_Code_of_Conduct_for_the_Responsible_Practice_of_Research.pdf

The document outlines the Institute's code of research conduct. Seeking knowledge, and imparting this knowledge, are fundamental functions of higher education. It follows from the right to pursue knowledge that researchers working under the auspices of WIT1 have a moral obligation to society as well as an obligation to the Institute to perform proper (ethically conducted) research and to communicate its outputs to their peers and, as appropriate, to the wider general community.

WIT embraces the traditional principles of academic freedom and recognises that members of Institute community, whether working collaboratively or individually, shall have, within the law, the freedom to question and test received wisdom, to put forward new ideas and to state controversial or unpopular opinions.

Open Research and sharing of knowledge are core to the ethos of the Institute.

This policy concerns published research (research paper, book chapter, monograph, dataset, software, or other artefact) that has one or more WIT-affiliated authors. This affiliation applies to any member of staff who is research active, or any member of the student body, whether they are postgraduate or undergraduate.

The aim of this policy is to maximise the return on investment of public money in research carried out at the Institute and it brings the Institute into alignment with the National Statement on the Transition to an Open Research Environment.

To assist researchers in better understanding the area of Research Data Management and in meeting funders' requirements in devising a Data Management Plan (DMP)

The purpose of this guide is to assist researchers in better understanding the area of Research Data Management and in meeting funders' requirements in devising a Data Management Plan (DMP). An increasing number of national and EU funding agencies and schemes such as EU Horizon Europe require researchers to develop a detailed plan for managing, storing or preserving data, sharing their data with the general public and the secure destruction of data following relevant retention periods. Devising a Data Management Plan is also good research practice for you and your wider research team even when the data cannot be shared for various reasons - legal, privacy, secondary use.

Waterford Institute of Technology (WIT) is responsible for the processing of a significant volume of personal information across the organisation.

It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

It is the responsibility of each Function to ensure personal information is processed in a manner compliant with data protection legislation and guidance.

The Institute has an appointed a Data Protection Coordinator who is available to provide guidance and advice on data protection issues and concerns.

All Staff must appropriately protect and handle information in accordance with the information's classification as set out in 6.1 below.

This Policy shall not give individuals additional rights greater than those allowed for under the General Data Protection Regulation (GDPR) or Data Protection Act 2018.

The objective of this Data Protection Policy (Policy) is to set out the requirements of the Institute relating to the protection of Personal Data where it acts as a Data Controller and / or Data Processor, and the measures the Institute will take to protect the rights of Data Subjects, in line with GDPR legislation, and the Data Protection Act 2018.

Annex II – Centre Tecnologic de Telecomunicacions (CTTC)

CTTC recognizes the great value of research data and data sharing in order to promote research work, publications and the institution's contribution to research, being always committed to pursuing the highest standards, and thereby support the development of a global research community in which research data is widely shared. -

The purpose of this policy is to:

- Provide guidance and support to all CTTC's researchers on the responsible management and protection of research data.
- Ensure that research data is stored, retained, accessed, and disposed of securely in accordance with all legal, statutory, ethical, contractual, and funding requirements, and
- Endorse the CTTC's Data Privacy Policy and Code of Conduct, and require all its researchers to adhere to them, as well as considering any other data management guidelines or requirements that may apply.

This policy applies to all CTTC staff engaged in research. The Policy also applies to anyone working in the institution, including casual workers, visiting researchers, undergraduates and taught postgraduates whose research findings are included in published research outputs, associates, consultants, agents or contractors undertaking research under the auspices of CTTC, using the institution's facilities on the University's premises anywhere in the world, or elsewhere on behalf of the University.

Research data is to be stored and made available for use in a suitable repository or archiving system, and whenever possible, provided with persistent identifiers.

It is important to preserve the integrity of research data. Research data must be stored in an accurate, complete, unadulterated, and reliable manner. Furthermore, they must be identifiable, accessible, traceable, re-usable, and whenever possible, interoperable, and made available in a timely way with as few restrictions as possible.

Research data is to be stored, made available and assigned a license for open use in compliance with legal, ethical, and contractual requirements, and providing no funder, third-party or contractual rights prohibit it.

Research data of future historical interest and the administrative records accompanying research projects should also be archived.

Research data is a legitimate product of research and must be cited as such adhering to scholarly norms; re-used data must be explicitly traceable and original sources acknowledged.

Research data should also be archived for as long as they are of value to the researcher and the wider research environment, and as long as specified by the funding agency, patent rules, legislation, embargo requirements and other regulatory requirements. The shortest storage period for research data is five (5) years after publishing/publication unless otherwise determined by law. In most cases, research data will be kept longer than the minimum five-year requirement. In general, research data should be made accessible at the earliest possible time, but only after the research team's first right of use period.

When research is supported by a contract/agreement/scholarship containing specific provisions on ownership, storage of- and access to research data, the provisions of such an agreement/contract will take precedence.

In the case of research´s data and records are to be deleted or destroyed, either after expiration of the required archive duration or for legal or ethical reasons, such action will be carried out only after considering all legal and ethical perspectives. The interests and contractual stipulations of third-party funders and other stakeholders, employees and partner participants in particular, as well as the aspects of confidentiality and security, must be taken into consideration when decisions about retention and destruction are made. Any action taken must be documented and be accessible for possible future audit.

CTTC recognizes the benefits of making Research Data accessible to the public or wider academic community.

Before sharing Research Data during or after a project it is essential to consider whether this is permissible considering IPR ownership, ethical, privacy, confidentiality requirements or any legal, regulatory, or funding restrictions. In addition, Researchers must consider whether Research Data has commercial potential and in consultation with the CTTC Legal Services consider if it is suitable for protection and/or transfer under CTTC's Intellectual Property Regulations

Access to Research Data during course of a research project should be restricted to the collaborators on the research project in the first instance and only made available to other parties if none of the issues are present (or have been managed, such as through anonymization of the Research Data and the preparation of a data access agreement for signing by the potential recipient of the Research Data) and with the permission of the research collaborators

To assist in complying with CTTC's obligations related to access to Research Data which is deposited in the Repository may be restricted or embargoed by technical means. Researchers who deposit Research Data in a national or international repository must only do so if the matters set out have been addressed and there are no restrictions in place governing the sharing of data.

Researchers are required to complete a Research Data Management Plan (DMP) for each new research project.

The Research Data Management Plan will set out:

a) The location/s where the research data and materials will be stored.
b) In what form the research data and materials will be stored (identified, coded, de-identified), the location of the code key or identifiers, if any, and risk management strategies regarding avoidance of possible re-identification.
c) The duration for which research data and materials will be stored and the reason for the nominated duration.
d) Custodianship, and details of who will have access to the research data, identifiers, and materials, including any third parties, and limitations of their rights to access
e) Ownership of the research data and materials, and limitations or restrictions applying to access, storage, disposal, sharing and re-use of data.
f) Whether the research data and materials are required to be submitted to an external party.

Researchers must submit their Research Data Management Plan online. Where a research project includes multiple researchers, the first-named researcher is responsible for completing and submitting the Research Data Management Plan on behalf of the research team.

Researchers are responsible for:

- Management of research data in adherence with principles and requirements expressed in this Policy and ensuring the appropriate security and integrity of the data, compliance with confidentiality undertakings and data protection law, and respect for ownership of IPR.
- Collection, storage, documentation, access to, and archiving or proper destruction of research data and research-related records.
- Compliance with the general requirements of the funders and the research institution; special requirements in specific studies must be described in the Data Management Plan (DMP)
- Planning to enable, wherever possible, the future re-use of data. This includes defining usage rights after a study has completed, with the assignation of appropriate licenses, as well as specifying any data storage and archiving requirements.
- Compliance with all organizational, regulatory, institutional, and other contractual and legal requirements, both regarding research data, as well as the administration of research records; and
- Registering new research studies at the proposal stage to ensure appropriate institutional support.

- Research students and Supervisors have a special responsibility for ensuring that candidates and students attend courses and manage research data according to the above guidelines. This means that all scientists and students must develop and document clear procedures for gathering, storing, archiving, using, reusing, accessing and storage or destruction of research data in connection with their research. This should include division of responsibilities in collaborative projects with other institutions. The information should be described in a data management plan (DPM).

The Principal Investigators (PI) should ensure the data management plan or the research proposal upon which the data management plan should be based addresses the matters set in this Policy and takes into account the requirements of collaborating parties.

CTTC is responsible for:

- Empowerment of organizational units, providing appropriate means and resources for research support operations, the upkeep of services, organizational units, infrastructures, and researcher education.
- Support of established scientific practices from the beginning. This is possible through training, education, support, and monitoring, while in compliance with legislation, regulations, third-party contracts for research grants, codes of conduct, and other relevant guidelines.
- Developing and providing processes and services for the storage, safekeeping, deposition, and registration of research data in support of current and future access to research data during and after the completion of research studies; and
- Providing access to infrastructures for data management planning, and the storage, safekeeping and archiving of research data and records, enabling researchers to exercise their responsibilities (as outlined above) and to comply with obligations to third-party funders or other legal entities.

Annex III - NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET (NTNU)

All data collected and processed by NTNU will be in compliance with privacy. They will be hosted at protected servers at NTNU and thus will be submitted to the compliance with the NSD, as well as to the General Data Protection Regulation. Data protection measures will be applied with regard to data collection, storage, retention, destruction, privacy and confidentiality. We will adopt a data minimization policy, collecting and processing only the data that is strictly necessary for running the activity. Participants will be informed about how and by whom data will be processed and stored and about their rights to access, modify and erase their personal data and about the procedures to enforce this.

The data collected during the project will be used only for the purposes of the project itself. Collected data will be protected through appropriate measures and will be effectively deleted when not needed any more for the project purposes or when requested by the data subjects. Best practices will be adopted for storage and destruction of data, in order to ensure that storage is secure and deletion non-reversible. The General Data Protection Regulation may require that, as well obtaining approvals from Data Protection Authorities, figures such as Data Controller and Data Processor are identified for the supervision and control of Data Protection and for the application of relevant legislation.

NTNU's employees have a personal responsibility to comply with the laws and regulations that apply at the university and to perform their work in an unselfish and ethically sound way.

NTNU is bound by the Ethical Guidelines for the Public Service. These Guidelines could be reachedat at "Code of ethics for NTNU employees": see https://innsida.ntnu.no/wiki/-/wiki/English/Code+of+ethics+for+employees+at+NTNU

The research ethics committee at NTNU is set as following:

https://innsida.ntnu.no/wiki/-/wiki/English/The+Research+Ethics+Committee?_36_redirect=https%3A%2F%2Finnsida.ntnu.no%2Fwiki%2F%2Fwiki%2Ftag%2Fethics%3Fp_r_p_185834411_title%3DCollection%2Bof%2Bpersonal%2Bdata%2Bfor%2Bresearch%2Bprojects

NTNY Privacy policy is published here:

https://innsida.ntnu.no/wiki/-/wiki/English/Collection+of+personal+data+for+research+projects

https://www.nsd.no/en/data-protection-services

Annex IV - EBOS TECHNOLOGIES LTD (EBOS)

EBOS Technologies has prepared a detailed data protection policy for the 5GMEDIAHUB project that includes the procedures for data collection, storage, protection, retention and destruction.

TYPES OF PERSONAL DATA:

EBOS Technologies will process during the lifetime of the Project different types of personal data such as name, e-mail address, telephone number.

PURPOSES OF PROCESSING:

EBOS Technologies will process personal data for the purposes of the 5GMEDIAHUB project, which has received funding from the European Union's H2020 research and innovation programme under grant agreement No.786886. The processing is necessary for scientific research purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects.

Particularly, EBOS Technologies will process personal data:

- of the personnel of the Consortium Parties (researchers) for the purposes of communication, interaction, information sharing and management of the Project.

LEGAL BASIS FOR PROCESSING:

The legal bases for processing is the performance of the 5GMEDIAHUB Consortium Agreement and of the 5GMEDIAHUB Grant Agreement with respect to the processing of names, e-mail addresses and telephone numbers of the personnel of Consortium Parties.

RECIPIENTS – TRANSFER TO NON-EU COUNTRIES:

a. The information will be available amongst the Parties of the Consortium.

b. Personal data may be transferred to the Swiss partner (IOM) and the partner from the UK (CENTRIC). All necessary safeguards will be implemented, and the transfer will take place in accordance with the GDPR requirements for data transfer outside the European Union.

STORAGE/RETENTION PERIOD:

The personal data will be processed until the purpose of the processing is served and, in any case, no longer than 5 years after the termination of the project according to the 5GMEDIAHUB Grant Agreement. The information is stored securely as described below.

DESTRUCTION PROCESS:

The personal data will be permanently deleted at the end of the storage period following the institution's internal destruction policy.

PROTECTION/SAFEGUARDS:

EBOS Technologies ensures that both physical and technical measures will be taken for the protection of the personal data which are going to be collected during the lifetime of the project. Only the necessary personal data will be collected in accordance with the data minimization principle.

The safeguards are the existence of the Ethical Advisory Board that has been established for the project, and internal policies of the organization.

RIGHTS OF THE DATA SUBJECTS:

Data subjects have the right to:

- Request information about whether EBOS Technologies holds personal information about them, and, if so, what that information is and why we are holding it.
- Request access to their personal information. This enables the data subjects to receive a copy of the personal information we hold about them and to check that we are lawfully processing it.
- Request rectification of the personal information that we hold about them. This enables the data subjects to have any incomplete or inaccurate information we hold about them corrected.
- Request erasure of their personal information. This enables the data subjects to ask us to delete or remove personal information where there is no good reason for us continuing to process it.
- Request the restriction of processing of their personal information. This enables the data subjects to ask us to suspend the processing of personal information about them.
- Request transfer of their personal information in an electronic and structured form to them or to another party (right to "data portability"). This enables the data subjects to take their data from us in an electronically useable format and to be able to transfer their data to another party in an electronically useable format.
- Object to the processing of personal data concerning them, on grounds relating to his or her particular situation.
- Lodge a complaint with a supervisory authority.
- In cases of consent, withdraw their consent at any time. Once EBOS Technologies has received notification that the data subject has withdrawn his/her consent, the company will no longer process the personal information for the purpose/purposes the data subject has originally agreed to. The withdrawal has future effect provided there is no legal reason for the reason to be processed.