HORIZON 2020 - ICT-14-2016-1

AEGIS

Advanced Big Data Value Chains for Public Safety and Personal Security

"Tackling ethical issues in a H2020 Project in the Big Data domain"- AEGIS Ethics White Paper

Author(s): Marina Da Bormida (Member of the EAB), George D. Karagiannopoulos (Member of the EAB) and Gert G. Wagner (Member of the EAB)

First Author: Marina Da Bormida

Dissemination level: Public **Nature:** Ethics

Internal Reviewers: Yury Glikman (Fraunhofer), Maurizio Megliola (GFT)

AEGIS KEY FACTS

Topic:	ICT-14-2016 - Big Data PPP: cross-sectorial and cross-lingual data integration and experimentation
Type of Action:	Innovation Action
Project start:	1 January 2017
Duration:	30 months from **01.01.2017** to **30.06.2019** (Article 3 GA)
Project Coordinator:	Fraunhofer
Consortium:	10 organizations from 8 EU member states

AEGIS PARTNERS

Fraunhofer	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
GFT	GFT Italia SRL
KTH	Kungliga Tekniska högskolan
UBITECH	UBITECH Limited
VIF	Kompetenzzentrum - Das virtuelle Fahrzeug , Forschungsgesellschaft-GmbH
NTUA	National Technical University of Athens – NTUA
EPFL	École polytechnique fédérale de Lausanne
SUITE5	SUITE5 Limited
HYPERTECH	HYPERTECH (CHAIPERTEK) ANONYMOS VIOMICHANIKI EMPORIKI ETAIREIA PLIROFORIKIS KAI NEON TECHNOLOGION
HDIA	HDI Assicurazioni S.P.A

Disclaimer: AEGIS is a project co-funded by the European Commission under the Horizon 2020 Programme (H2020-ICT-2016) under Grant Agreement No. 732189 and is contributing to the BDV-PPP of the European Commission.

EXECUTIVE SUMMARY

Big Data has tremendous potential to be exploited for the public good and data-driven innovation brings significant benefits. Last but not least, this is the case because data represents the raw material for most AI technologies.
Nevertheless, Big Data technologies and their use also imply a number of ethical concerns, risks and challenges. It is therefore paramount to adopt adequate mitigating measures and safeguards, also in relation to the research and demonstration activities of European projects, as well as to their achievements.

This Ethics White Paper (EWP), capitalizing on AEGIS experience, is aimed at offering a focused and practical guidance and best practices for dealing with ethical issues in Big Data projects, proposing ways of progressing the action and developing research results in a constructive and ethically-compliant manner.

This document, therefore, provides an overview of how beneficiaries in the data-driven domain can operationalize responsible research and innovation principles, ethical guidelines and data ethics in the framework of their action, providing best practices and lessons learnt on how reflecting ethical considerations in their activities and results.

It is aimed at offering suggestions and tips for getting project development and outcomes 'ethics-compliant' under Horizon 2020 and the applicable regulatory framework (international, EU and national law), by mitigating some of the mentioned risks, in terms of the privacy and ethical challenges associated with Big Data use.

The Ethics White Paper (EWP) consists of two parts:

- the first part contains a set of lessons learnt, best practices and recommendations on how to deal with ethical issues raised by H2020 Projects in the Big Data domain. This part capitalizes on AEGIS experiences, and covers the different development stages of an H2020 project, starting from the proposal, till the further uptake/exploitation of project's outcomes after project's end;
- the second part is project-specific and refers to the ethics-related work and assessment, as conducted in the framework of the project "AEGIS - Advanced Big Data Value Chains for Public Safety and Personal Security".

Table of Contents

1. INTRODUCTION

Big Data technologies, if designed, developed and applied in a responsible manner, have significant potential to be exploited for the public good, being able, for instance, to harness the real-time and predictive analytics for enhanced decision making, to provide anticipatory paths towards risk management and new fashions to optimize value chain dynamics. Such developments are capable of offering major business opportunities for European industry and the whole society. This is the case especially, as generally recognized, because data represents the raw material for most AI technologies.

Besides all the benefits of data-driven innovation, the same also implies a number of ethical concerns, risks and challenges. Large-scale data collection and processing amplify risks to privacy, fairness, egalitarian treatment, and due process, potentially leading to biased decision-making (if based on biased or inaccurate data samples). Big Data is exposing individuals and society to the risk of data monopolies as well as discrimination, manipulation, misuse, asymmetries of power, increase of digital divide and dataveillance or even technological determinism.

Despite these aspects, data-empowered applications and services remain neutral and it is unquestionable that Big Data brings promising potentialities. It is therefore paramount to adopt adequate mitigating measures and safeguards for supporting their responsible deployment and operation. These remarks are relevant also in relation to the research and demonstration activities of European project in the Big Data sector, including above all H2020-funded actions, as well as to their achievements.

This document provides some suggestions and tips on how H2020 beneficiaries in the concerned domain can mitigate some of the mentioned risks, in terms of the privacy and ethical challenges associated with Big Data use. At the same time, the document suggests an approach where any risks to individual privacy should be weighed against the benefits of using data-based technology to improve livelihoods and, in some cases, save lives.

The EWP is structured in two parts:

- the first part consists of a set of lessons learnt, best practices and recommendations on how to deal with ethical issues raised by H2020 Projects in the Big Data domain, capitalizing on AEGIS experience, and covering the different development stages of a European project, starting from the proposal till the post-project phase;
- the second part is project-specific and refers to the ethics-related work and assessment as conducted in the framework of AEGIS project.

2. RECOMMENDATIONS, BEST PRACTICES AND LESSONS LEARNT FOR DEALING WITH ETHICAL AND LEGAL ISSUES IN A EUROPEAN BIG DATA PROJECT

2.1. PROPOSAL PHASE

It is crucial to consider ethical issues starting from the conceptual stage of a proposal: this can improve the quality of research and foster its better alignment with social needs and expectations, paving the way for building a collaborative and constructive relationship between the research initiative and ethics fulfilment.
This approach is expected to facilitate societal acceptance of the final outcomes of the projects, thanks to the increase of public trust, generated by the respect of high ethical standards.
Being ethics an integral part of all research activities funded by the European Union, as stated by the relevant legal background[1], the European Commission (EC) set an Ethics Appraisal Procedure, which is the process to assess and address the ethical dimension of activities funded under Horizon 2020.
According to the first step of this procedure, at the stage of submitting project proposals, applicants must describe the ethically relevant issues of their project and demonstrate how these issues will be taken into account and handled in the envisaged project. The aim is to ensure compliance with key ethical standards and applicable institutional, regional and national procedures of the respective organisations within research projects.
In particular, applicants are required to conduct the so-called "Ethics Self-Assessment" in this phase: they have to fill in the Ethics issues table and, in case some ethical issues arise, to prepare the Ethics section in Part B of the proposal (usually Section 5 of the H2020 Programme Proposal Template 2018-2020), where to demonstrate awareness of ethics issues and describe how they intend to address them in the project.
In case of ethical issues, a good practice is not only to describe them in Section 5 (which is not covered by page limits), but event to take them into account in several other parts of the application (objectives, methodology, impact, risk assessment,…). Such considerations should demonstrate compliance with national and EU legislation and, when applicable, provide details on the procedures for acquiring necessary authorisations/permits/approvals and submitting existing documentation. In Big Data projects, usually the main ethics issues arising are related to "Humans" and "Personal Data", though in some cases other may occur (such as "Misuse" and "Third Countries").
In case of researches involving processing of personal data, there is a number of relevant measures to be taken or simply opportune, such as, depending on the specific context, the involvement of the Data Protection Officer (DPO), the provision of details on informed consent procedures and on the security measures to prevent unauthorised access to personal data. Other possible measures include the provision of details of the methods used for tracking, surveillance or observation of participants, and of details on the pre-existing datasets or sources, merging existing datasets (in case of further processing of previously collected personal data), and other.

[1] Art. 14, Horizon 2020 Regulation (EU), N. 1290/2013, Rules for Participation; Art. 34, Model Grant Agreement; Art. 19, Regulation (EU) No 1291/2013, establishing Horizon 2020.

In case of complexity or multiple issues raised by the proposal, a good practice is to incorporate ethical issues into a dedicated Work Package (WP) or explicit tasks, which allow a better integration of ethics work into the daily research activities. In such cases, it will be also opportune to plan the appointment of an Independent Ethical Expert or of an Ethical Advisory Board, clearly describing its role and tasks in the management structure of the proposal.

2.2. PROJECT DEVELOPMENT PHASE

Ethics, legal and societal issues are mostly raised, on the one hand, in relation to the implementation of the research activities and to the generated results, and, on the other hand, in relation to the operations in the demonstrators/pilot cases and validation activities.
The design, development and validation of a data-driven system or application or service in the framework of a H2020 project has to be conducted in a responsible way, protecting human rights and ethical values and fostering positive societal impact. This achievement can be realized only if the Consortium is aware of the role of ethical and legal issues during and after project development and is committed to compliance.
The following description is intended to provide a snapshot of lessons learnt, recommendations and best practices, based on the ethics experience matured within FP7 and H2020 projects in this and related domains, including AEGIS.

2.2.1. Legal review

At the beginning of the project it is recommended to conduct a legal analysis, to clearly set out the relevant legal and ethical framework with which its tools and operations must comply.
Particular attention should be devoted to privacy and data protection law, with the objective to ensure that requirements arising from this kind of law are embedded in the technological solutions from the design stage on, as required by "privacy by design and by default" paradigm. In fact, in most of Big Data projects, the use of technologies could potentially interfere with the right to privacy and the protection of personal data. It is, therefore, essential to analyse the relevant regulatory framework concerned and provide safeguards against the potential pervasiveness of such solutions and their use, in order to design and develop them in a privacy-friendly fashion. The key legal instruments relevant to Big Data Projects are aimed to guarantee the individuals' sphere of autonomy within which to operate. For this purpose, they define a number of legal values and principles -foreseeability, accountability, legality, necessity, proportionality and transparency and other- and contain a set of substantial safeguards and countermeasures against the spread of technologies resulting in an unfettered surveillance.
Besides the national regulatory systems (especially of the countries where pilot/validation activities will be performed), the privacy and data protection European regulatory framework must be considered, including for instance:

- Regulation 2016/679/EU (GDPR)
- European Convention of Human Rights
- Charter of Fundamental Rights of the European Union
- Directive 2002/58/EC "ePrivacy Directive"

In addition to legal provisions and principles, it is important to refer also to ethical and social oriented values, being the "privacy in law" concept strongly interconnected with them, as well as to the European Courts' case law, which is very helpful for partially filling the gaps and pitfalls that can be found in legislation. Likewise, also the guidelines and recommendations set by European-wide initiatives, like BDVA (Big Data Value Association, http://www.bdva.eu/), should be taken into account.
It is, therefore, strongly recommended to take all this set of variables into account in a systematic way, so that to be able to answer key questions, such as why privacy matters in the project's implementation and final system and how it should be safeguarded.

2.2.2. Legal and Ethical Strategy

Project Consortium is strongly recommended to elaborate the Ethical and Legal Strategy or Policy in the first month of the project. It is intended as a comprehensive framework on legal, ethical, and, often, societal issues, including also data protection, privacy and IPR handling, functional to drive the design, deployment and validation of the technical solution. It should also set ethics management procedures and conduct a thorough analysis of the ethics issues raised by the project, besides pointing out the measures that will be taken to ensure compliance with the ethics standards of H2020 and regulatory system.
In particular, it usually serves:

i) to report the finding of the legal review, defining the EU and national regulatory framework driving the project's solution;
ii) to provide an overview of project's solution and its components, focusing on portions of the system processing personal data (if applicable), as well as representing the purpose of such processing and describing the origin of personal data and its collection method;
iii) to elicit the legal, data protection and ethical requirements, providing input to the use cases, the architecture and specification task and specifying the measures to cover these requirements for data protection;
iv) to assess to what extent they have been taken into account during project implementation and within the final system;
v) to define ethics roles, procedures and a roadmap for activities related to ethical issues and procedures.

The strategy must be strictly interrelated with the overall project implementation and final achievements, being aimed at providing the basis for the main guidelines that the Consortium will have to respect towards ethics, privacy and data protection. It should offer practical indications and hints on how to address ethical issued raised by the project, detailing methods, tools and processes, as well as providing responsible research ethics guidelines for project purposes. For instance, guidelines should be provided, in case of involvement of voluntary participants in the demonstration activities, on the recruitment procedures and on the implementation of the informed consent procedures, as well as and on the way in which the voluntariness of consent will be guaranteed to participants in a position of dependence and vulnerability.
The strategy should be updated during project's lifecycle, according to project's progress.
An advisable approach is to split the Strategy in two main parts:

- One of the part should be dedicated to the project's implementation phase, establishing ethics procedures, depicting the role of the Ethics Advisory Board or Independent Ethics Expert (if appointed), defining the roadmap of the ethics-related work, analysing the demonstrators/pilots/use cases and setting specific ethics and legal requirements referring to their operation;
- Another part should be dedicated to project's solution and its components, including the chosen methodology underlying the ethical work, as well as identification of the key principles, legal evaluation and preliminary assessment of project technologies. This part should also include the findings of the regulatory review, the description of key principles relevant to project's solutions and the elicitation of the legal, data protection and ethical requirements.

Comprehensive framework for identifying and tackling with legal and ethical issues, including Privacy & Data Protection. It is aimed at driving project's research activities, results and validation in a ethically and legal compliant manner, pointing out safeguards and mitigating measures, as well as setting ethical and legal requirements. The Stratey should be updated during project's lifecycle. A good approach is to split it into two main parts, respectively addressing project's implementation phase and project's solution

2.2.3. Awareness and training session

In case that all or some project partners are unfamiliar in dealing with ethical issues, or where issues are particularly complex, a good solution is:

- to raise their awareness, especially of the leaders of all relevant work packages, on salient aspects of the project's impact on society and ethical dimensions;
- to organize training courses on research ethics and ethical issues and on how to tackle with them, including practical guidance.

In some cases, it can be opportune also to prepare and circulate to them a Data Protection Handbook.

> In case the project partners are unfamiliar with dealing with ethical issues, or where issues are particularly complex, it is advisable to organize awareness and training sessions, as well as to circulate a Data Protection Handbook

2.2.4. Prioritization Paradigm for balancing opposite interests

In line with the findings expressed by the European Group on Ethics in Science and New Technologies[2], it is advisable to go beyond the traditional drastic trade-off between opposite interests and goals at stake, such as security/safety and freedom (including the right to privacy), and to adopt a Prioritization Paradigm.
The EGE Group remarks that human dignity "is the core principle of the European moral framework, and as such it cannot be traded off". On the other hand, the right to privacy and the right to data protection, as well as the right to information and transparency, are not absolute rights. Therefore, such rights must be balanced against other rights of other persons or groups. Some kind of balancing, weighing, or choice between priorities is necessary, in the meaning of need to find an equilibrium between rights of persons and rights among persons. Competing interests can be related, for instance, to, on the one hand, competitiveness, growth and jobs, public safety and personal security, and, on the other hand, privacy, data protection, informational self-determination, and individual freedoms
In this regard, a rich jurisprudence of the European Court on Human Rights and the Court of Justice of the European Union (ECJ/CJEU) has repeatedly stated that a balancing exercise with other rights is required when applying and interpreting Article 8 of the Charter of Fundamental Rights, setting forth the right to the protection of personal data.

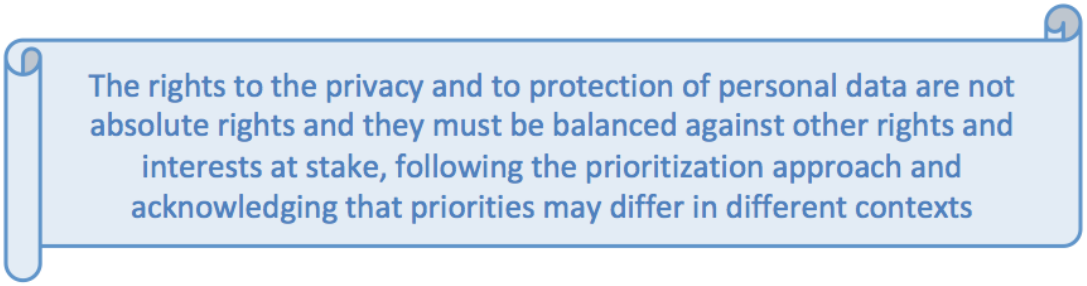
This is also linked with the principle of proportionality, expressly recognized by the Recital 4 of GDPR: "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".

This need for equilibrium and balancing is important for H2020 project technologies as well, including their legal evaluation and assessment.

The project partners are invited to concretely operate in line with the prioritisation approach, not giving up on any of the rights and interests and, finally, acknowledging that priorities may differ in different contexts (in particular the different sectors and application context). The project Ethical and Legal Strategy, including requirements, should be conceived and

[2] "Ethics of Security and Surveillance Technologies", Opinion n. 28 of the European Group on Ethics in Science and New Technologies, 2014.

implemented, both during project life and in the post-project phase, in a way consistent with this paradigm.



2.2.5. Ethical and Legal Requirements

It is advisable to elicit the legal and ethical requirements, including also privacy, data protection and, if relevant, IPR handling. The requirements are guidelines on how to conceive, develop and use project's architecture and tools in an ethical and legal compliant way, without forgetting checkpoints. They provide input to the use cases, the architecture and specification task. It is opportune also to specify the measures to cover these requirements.
The requirements can be elicitated according to different approaches. One of the most useful is the Privacy-by-Design, combined with the Privacy Protection Goal:

- Privacy by Design addresses the design of the technical system, as well as the business processes, and relies on the idea that there is the need of putting privacy principles into the design process of data processing systems since the very beginning. It is recommended to adapt to project's peculiarities the seven principles to be considered in the design process, as conceived by Cavoukian: "1. Proactive not reactive – preventative not remedial 2. Privacy as the default setting 3. Privacy embedded into design 4. Full functionality – positive-sum, not zero-sum 5. End-to-end security – full lifecycle protection 6. Visibility and transparency – keep it open 7. Respect for user privacy – keep it individual and user-centric".
- Privacy Protection Goal, on the other hand, recognizes a key role to the private individual's point of view. It considers the protection goals as central elements for deriving requirements to be complied with in system design, as well as for identifying risks and countermeasures and in an evaluation perspective. Besides the well-known security protection goals, named "Classic CIA Triad" (consisting of confidentiality, integrity, and availability), three further specific privacy protection goals are encompassed: unlinkability, transparency and intervenability. The protection goal approach promotes the balance of the privacy and security requirements against other protection goals.

As mentioned above, it is advisable to make use of a holistic approach in setting requirements. Therefore, besides GDPR-setting out data subjects' rights and providing general rules on the lawfulness and fairness of the processing of personal data-, other legal instruments and ethical instruments should be applied, such as the European fundamental rights framework and the national legislations applicable on a case-by-case basis, as well as ethical standards and highlights of strategic initiatives, like BDVA.

It is also recommended to update and refine the requirements on the basis of project progress, as well as to integrate their detailed description with a presentation in table format. An example of this format is the following.

Number	Short name	Description	Assessment method	Phase	Notes

Some examples of requirements:

- Assignment of responsibilities
- Use of private environment/cloud as much as possible
- Data minimization
- DPO's confirmation
- Data Protection Impact Assessment
- Recruitment procedures
- Informed consent procedures
- Data Quality, including Data Accuracy and Data Security
- Accountability
- Application scrutiny to local/national boards (if required by national legislation concerned)

The legal and ethical requirements, including also privacy, data protection and, if relevant, IPR handling, are guidelines on how to conceive, design, develop and use project'system and tools in an ethical and legal compliant way. A good approach for their elicitation is the Privacy-by-Design, combined with the Privacy Protection Goal. It is recommended to present such requirements in a table format and to specify the measures to cover them, as well as to proceed to their update and refinement according to project progress.

2.2.6. Appointment of the Ethics Expert or of the Ethics Advisory Board

The "Ethics Advisory Board" (EAB) or the "Ethics Expert" (EE) has the role to give advice to a project and thereby facilitate and complement existing oversight regimes by competent ethical and legal authorities. Its appointment is useful when ethical issues arise and the project partners are unfamiliar with dealing with them, or when they are complex or sensitive.

They should interface with the Consortium, ensuring that the WP leaders of all relevant work-packages include in their work flows the processes needed to make their project solutions and activities compliant with existing EU and national legislations and H2020 ethical guidelines.
If necessary, the EAB or EE raises awareness by the Consortium on ethical and legal issues and societal dimensions of the action.
The members of the EAB or the EE are external experts and practitioners, selected among subjects with proven credibility, impartiality, morality and experience in the given field of scientific research and pilots. It is advisable that a EAB will meet regularly, physically or via conference call. The EE or the EAB is in charge of the ethical oversight of the project research activities, outputs and experiments, assesses project solutions with respect to privacy-friendliness and provides independent opinions and thoughts. The EAB or EE periodically reports to the Commission on the implementation of ethical principles in the project as well as on compliance with applicable national and EU regulations.
The EAB or EE should have access to deliverables and results generated by the Project Partners. They are expected to participate and/or contribute to project's workshops or meetings (when opportune) and to co-create and/or review selected parts of the ethics and privacy related deliverables.

In some cases it is advisable to appoint an independent Ethics Expert or an Ethics Advisory Board, that is in charge of the ethical oversight of the project research activities, outputs and experiments, assesses project solutions with respect to privacy-friendliness and provides independent opinions and thoughts. The EAB or the EE periodically reports to the Commission.

2.2.7. Data Protection Officer of the project

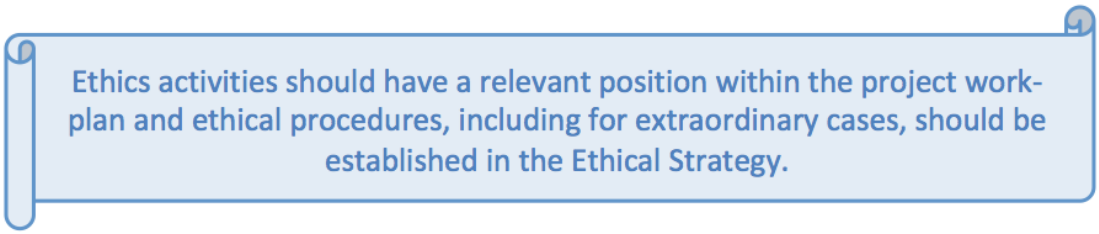
A best practice is to appoint, at the beginning of the project, a Data Protection Officer (DPO) for the project for the handling and management of personal data in accordance with the existing provisions of GDPR and other relevant EU and national legislations.
The responsibilities of the DPO should be in line with Article 39 of the GDPR.

If the project collects and processess personal data, it is recommended to appoint a Data Protection Officer, whose responsibilities should be in line with Article 39 of the GDPR.

2.2.8. Ethics activities and procedures

Ethics activities should have a relevant position within the project workplan and be functional to ensure that ethical principles as well as regulatory compliance are met throughout the project.

For this purpose, ethical procedures should be established and implemented and the Ethical Strategy and continuously updated.
It is advisable to set extraordinary procedures, to be followed in case of ethical issues. For instance, in such a case, partners are encouraged to consult:
1) at first, their own ethics departments;
2) in a second time, the Ethics Expert or the Ethics Advisory Board (if existing)
The partners are recommended to adhere to the recommendations and indications of ethics departments and/or of the EE or EAB and implement the adequate mitigating actions, countermeasures necessary in order to reinforce ethical safeguards and fully comply with both ethical standards/best practices and regulatory obligations or constraints.



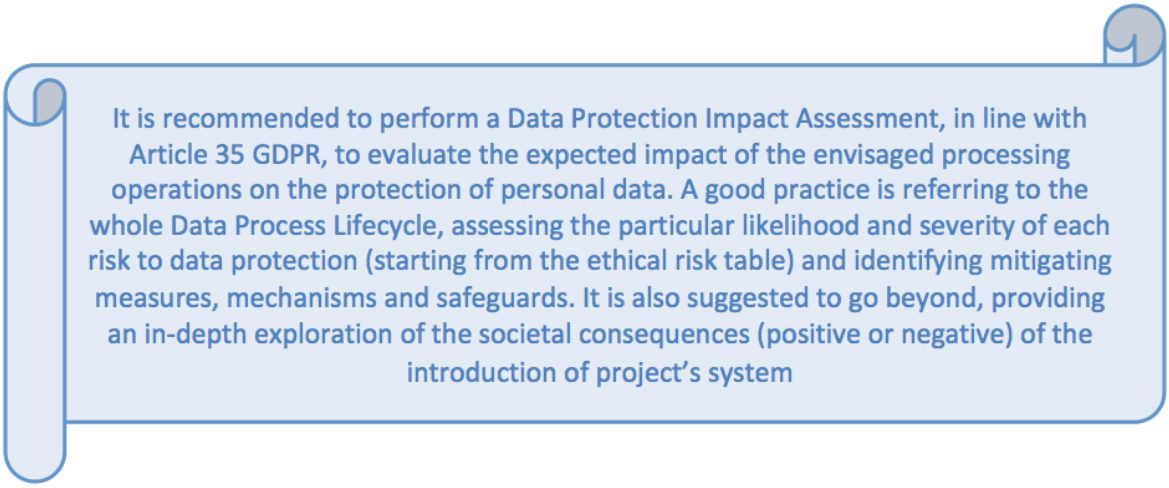
2.2.9. Ethics Workshops

Another good practice consists in organising some internal and/or public discussion or consultation with stakeholders on privacy and other ethics issues arising from the project research, also as part of the dissemination and public outreach activities.

2.2.10. Data Protection Impact Assessment (DPIA)

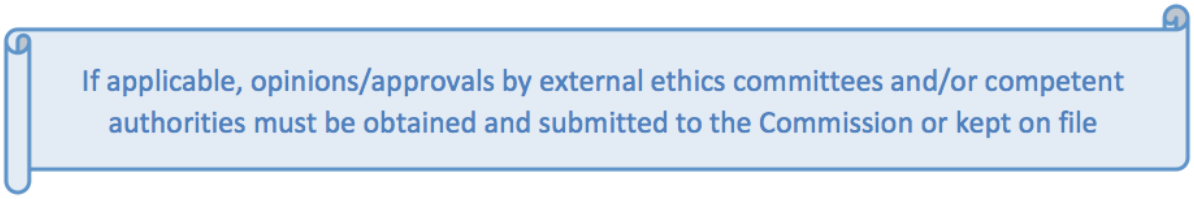
The DPIA should be strictly correlated with the Ethical and Legal Strategy and its list of requirements. Lingering over the DPIA, the mid-term and final ethical assessment of project's operations, framework and architecture could be elaborated, in particular within the ethics report, assessing to what extent the legal and ethical requirements have been taken into account and offering recommendations.
The assessment should refer to the Data Process Lifecycle, from the collection, to preparation, input, processing and output phases.
It also should go beyond, providing an in-depth exploration of the societal consequences (positive or negative) of the introduction of project's system.
The DPIA should assess the particular likelihood and severity of each risk to data protection, taking into account "the nature, scope, context and purposes of the processing and the sources of the risk". The starting point should be the ethical risk table, usually inserted into the proposal and updated during the course of the project.
The impact assessment is also expected to include "the measures, safeguards and mechanisms envisaged for mitigating each risk, ensuring the protection of personal data". The key questions driving the DPIA should include the following: what is gained, what is lost, by

whom, how is this framed and measured and shared, by whom, and how is this articulated to decision-making processes related to project's technologies?
The DPIA Framework is going to comprise the assessment of the pros as well as the cons of project's technologies in general and of demonstrators' applications. The impact assessment should conduct balancing assessment, between, on the one hand, privacy/data protection tensions and, on the other hand, societal expectations and public interests related to given domain.
In relation to DPIA, it is useful to mention Article 35 of the new Regulation. It indicates that "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".



2.2.11. Opinions or approvals by ethics committees and/or competent authorities

If applicable, opinions/approvals/permission by external ethics committees and/or competent authorities for the research with humans and/or data collection and processing at the trial sites/locations must be obtained and submitted to the Commission or kept on file.



2.3. POST-PROJECT PHASE

This section provides a set of high level recommendations, lessons learnt and guidelines to the relevant stakeholders for the best uptake and exploitation of Big Data solutions generated within European projects (but mostly applicable also to other technological developments developed in other framework, for instance within the research department of a company or in

a value chain). They are also relevant for the further enhancement or extension of such Big Data solutions, in order to adapt them to other application contexts, with specific needs and requirements.

The provided lessons learnt and recommendations are also based on the experience of the AEGIS Consortium, which designed, developed and tested a data-driven system taking into account to a great extent ethics, privacy, data protection issues and societal mandates.

The recommendations refer to:

- ethics, privacy and data protection;
- improvement of societal impact;
- further extension and enhancement of data innovative solutions developed within European Projects, like AEGIS system

Ethics, Privacy and Data Protection recommendations, guidelines and lessons learnt		
LL1	**Assignment of responsibilities**	Appointment and involvement of the Data Protection Officer, the Data Controller and data processors or sub-processors, in conjunction with a clear assignment of responsibilities to each of this figures/entities involved in the processing, in relation to the specific role covered. Each of them has to meet obligations and to follow specific principles.
LL2	**Privacy and Data Protection Policy**	Preparation of a handbook containing the Privacy and Data Protection Policy and distribution of it to the further uptakers of data-driven systems developed in a European Project (like AEGIS),. This Policy contains the main principles and practical, technical and organizational guidelines and practices to be followed in relation to privacy and data protection for system's operations, including also procedures for safeguarding data subjects' rights.
LL3	**Purpose limitation and safeguards against misuse**	Also in the post-project phase, data collection and processing through the system deployed in the project has to occur for the specific, explicit and legitimate purpose selected and, if applicable, communicated to the data subjects. Data has not to be further processed in a way incompatible with that purpose. Any appropriate safeguards against misuse should be taken.
LL4	**Compliance with European ethical principles and values**	The concrete implementation modalities of solutions developed within European projects must comply with the relevant ethics guidelines and principles. These include avoidance of harm and social sorting, transparency and feedback of information, the lawfulness and fairness principles, the purpose and proportionality principles, data quality and accountability principles and data storage principle. This will also contribute to minimize possible resistance to the adoption of the solution as a result of privacy concerns.
LL5	**Ethics and data protection training to the figures involved in the data collection and processing**	It is recommended that in certain circumstances (taking into account the application context's level of maturity), focused training sessions are organised, for the benefit of the individuals covering the key roles in data collection and processing. This can be profitably arranged throughout company/institution's Data Protection Officer. The training is functional to inform each of such figures on his/her respective obligations and on the principles and practices to be followed.

		The training could be conceived in addition or as an alternative to the Privacy and Data Protection Policy.
LL6	**Informed Consent Procedures**	The procedures for informing individuals about system's objectives, data gathering, handling and use have to be executed for the legitimate use of it in real environments, if other legitimate source of the processing are not applicable. The data subject's consent to the transmission and processing of his/her data is one of the criteria identified by the regulatory system (GDPR and other pieces of national and EU legislation). In order to be valid, the consent has to be unambiguous, specific, informed, free and timely given. Nevertheless, it is opportune to investigate also promising developments, such as automating compliance, sticky policies and dynamic user consent, especially in the use of APIs or Blockchain for smart contracting in data markets.
LL7	**Recognition and respect for data subjects' rights**	In the future use of data-driven technologies resulting from European projects, all the data subject's rights have to be granted. Data subject's rights include both the rights of information and the rights of intervention (where also rectification, erasure and data portability are relevant, as well as the chance to withdraw the consent).
LL8	**Technical and organizational measures to ensure security, integrity and confidentiality of data**	All the technical and organisational procedures have to be implemented to comply with art. 5 letter f GDPR in the post-project phase. According to this article, personal data shall be "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". The level of security has to be appropriate to the risk, taking into account "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" (art. 32 GDPR). In case of need, people who collect, use or access personal data must be subject to an enforceable duty to keep them confidential and secure, for instance through a confidentiality clause or NDA[3]. The access to data should be limited as much as possible: a good practice is to set a closed system's operators group, composed of only authorized persons, contractually obliged to follow the data security rules and fully committed to the strict rules of data access and disclosure. The use of authentication and authorisation infrastructure should be monitored on the basis of the concrete deployment circumstances, also through the involvement of the Data Protection Officer.
LL9	**Accountability**	Appropriate technical and organizational measures have to be put in place in order to be able to demonstrate compliance with the law, when requested. Such measures include, for instance, i) the appointment and involvement of a Data Protection Officer in the data processing planning and operations,, ii) the adequate documentation on what personal data are processed, how, to what purpose, how long, iii) documented procedures and processes directed to tackle with data protection issues at the design and operation stage and in case of response to a data

[3] Non Disclosure Agreement.

		breach.
LL10	**Customized Data Protection Impact Assessment**	A customized Data Protection Impact Assessment should be conducted before uptaking the data innovations. Such further assessment is directed to consider the concrete circumstances of the data processing and possible changes and/or adaptations developed on the solutions as generated by the project. It is compulsory, according to art. 35 GDPR, "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".
LL11	**Prior consultation of the supervisory authority**	"Where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk", according to Art. 36 GDPR, the controller shall consult the supervisory authority prior to processing. The Data Protection Officer can help in this assessment.
LL12	**Raising awareness**	Depending on the specific application circumstances, it can be useful to conduct awareness raising campaign, showing, on the one hand, the social benefits deriving from the use of the data-empowered solution at stake and, on the other hand, the intrinsic privacy-respectful nature of it.
LL13	**Stakeholders' consultation**	In case of introduction in the system of less privacy respectful features (for instance for meeting specific needs of the context situation in which the same will be used), it may be useful to apply mechanisms for understanding and addressing citizens' concerns, like focus groups or public consultation.
R14	**Data minimisation**	It is recommended that any further improvement and customization of H2020 project's technologies adhere to the data minimization approach. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.
R15	**Privacy by Design and by Default**	It is paramount that Privacy by Design and by Default continue to be core of future extensions of any project's outcomes, in compliance with GDPR provisions.
R16	**Data storage minimisation**	In line with GDPR, "Personal data must be… kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed".
R17	**Use of private environment as much as possible**	Being privacy and control more easily retained in a private environment, they should be used when possible for the storage or processing of personal data, in order to retain bigger control of the data being processed.
R18	**Data anonymization**	Whenever possible, personal data should be immediately anonymised, for instance through local dedicated services for anonymization and filtering of data, striping them of any private or sensitive information.

3. AEGIS-SPECIFIC PART

3.1. AEGIS PROJECT: AN OVERVIEW

The AEGIS Project created a curated, semantically enhanced, interlinked & multilingual repository for public & personal safety-related Big Data, by bringing together the data, the network & the technologies to deliver a data-driven innovation. Such data–driven innovations and the AEGIS system enabling it are expected to expand over multiple business sectors and take into consideration structured, unstructured & multilingual datasets, rejuvenate existing models and facilitate organisations in the Public Safety & Personal Security linked sectors to provide better and personalized services to their users.

The action, by tackling some of the data-related challenges (such as the lack of collaboration and offerings based on fragmented and domain-specific data) was developed in order to improve the services of the Public Safety & Personal Security linked sectors (including public sector, insurance, environment, health, automotive, smart home, etc.), for more effectively providing innovative cross-domain services, able to cultivate more caring and danger mitigating practices. Therefore, the project's outcomes contributed, in a direct or indirect way, to enhance the welfare and protection of the general public and of individuals through prevention and protection from dangers affecting safety, such as accidents or disasters.
In light of this expected positive societal impact, in demonstrating and using the AEGIS system personal data were (partially) collected and processed, as well as participants involved in the demonstration activities were tracked and observed during evaluation.

Additional information on the project's objectives, activities and results can be retrieved at the following link: https://www.aegis-bigdata.eu/

3.2. ETHICAL AND LEGAL ACTIVITIES IN THE AEGIS WORKPLAN

In AEGIS project ethics and legal dimensions and activities were interrelated with the other tasks and with the overall project's workplan. In particular;

- WP9 "Ethics Requirements" referred to the activities and tasks to be executed according to the Ethics Screening:
    - Project-specific Data Protection Impact Assessment methodology (D9.1 "OEI - Requirement No. 1"). It approached the data protection and ethical issues in a comprehensive manner and especially considers the three demonstrators. This document explored the societal consequences (positive or negative) of the introduction of an AEGIS system and provided the assessment methodology functional to evaluate the compliance with ethics and data protection strategy and requirements, as described in D1.2 and refined in D1.3. It has served to AEGIS Ethics Advisory Board to concretely proceed with its ethics evaluation in both the evaluation cycles, in conjunction with the Ethics Strategy and its ethical and legal requirements.
    - Copy of the relevant opinion in relation to data collection and/or processing in the project (D9.2 "POPD - Requirement No. 3")
    - Periodic EAB's reports to the EC (M18 and M30) for timely ensure that the project was on the right tracks just before the completion of WP1 (AEGIS Data Value Chain Definition and Project Methodology and for the final ethics assessment.
- WP1" AEGIS Data Value Chain Definition and Project Methodology", especially T1.4 "Regulatory Framework for Data Protection, IPR and Ethical Issues". In D1.2 "the AEGIS Methodology and High-Level Usage Scenarios" the AEGIS ethics,

privacy, data protection and IPR strategy was outlined, whilst it was refined and updated in D1.3 "Final AEGIS Methodology". These deliverables referred to the regulatory framework and, above all, to the methodology/strategy elaboration for ethics, data protection and privacy issues, including ethics and data protection requirements. This ethics strategy and underlying methodology served as the basis for the main guidelines that partners had to respect towards ethics and privacy protection and overall ethics and regulatory compliance.

- Ethics-related activities were designed and conducted in WP3 "Work package title System Requirements, User stories, Architecture and MicroServices", WP4 "AEGIS Infrastructure Implementation and Rollout" and WP5 "AEGIS Data Value Chain Early Community Demonstrators".

3.3. ETHICS-RELATED WORK

During the whole course of the project, several activities were undertaken, both by the Consortium partners and by the Ethics Advisory Board (EAB):

- An AEGIS Ethical & Societal Board (ESB) was established and was fully operating and involved in the project's development, working in close collaboration with the partnership;
- Oversight and evaluation of the AEGIS's progress and results were conducted by the EAB, for supervising the operation of the project and ensuring that the developed solutions adhered to the relevant set of ethical and legal requirements.
- A specific Ethical, Privacy and Data Protection Strategy was elaborated at the beginning of the project (closely involving the demonstrators) and later updated;
- A set of ethical and legal requirements were identified, including privacy and data protection, as well as IPR handling;
- The Privacy by Design Approach, in conjunction with the Privacy Protection Goal paradigm was customized to project's features and followed in the course of its implementation, including the adherence to the "Need to know basis" principle and the proportionality principle;
- Legal compliance was ensured (GDPR and other applicable European and national rules)
- Recruitment and Informed Consent Procedures were followed;
- The EAB or one of its members participated to Ethics meetings/workshops;
- Liaison was established with e-Sides project (https://e-sides.eu/e-sides-project) and one of the Ethics Expert attended two of it workshops.

3.4. ETHICAL ASSESSMENT OF AEGIS

3.4.1. AEGIS Platform and Ethical Assessment at project level

The Consortium demonstrated high level of awareness, attention and knowledge in relation to ethical, privacy, data protection and societal implications, thereby conforming to the principles of responsible research and innovation, whilst paving the way for realizing a vibrant data-driven EU economy in the PSPS domain.

Both the system design and its development took privacy and ethics issues into account, by balancing operation between ethical, privacy and data protection requirements and the requirements of different nature (e.g. usability requirements, economic requirements). Proper safeguards, when necessary or opportune, were adopted.

The "need to know basis" principle and Privacy by Design and by Default approaches were followed in designing and implementing the technical solutions, in conjunction with the proportionality principle, integrating privacy-preserving technologies into AEGIS Big-Data solution (e.g. anonymisation, sanitisation, access control). AEGIS Blockchain powered Security, Privacy, Quality and IPR Data Policy Framework, and the Business Brokerage service relying on it, represent examples of practical implementation of the requirements and recommendations set forth in the AEGIS Ethical and Legal Strategy. The CloudTeams Anonymisation Tool was the main anonymisation tool chosen by the project: it is an extensible, schema-agnostic plugin allowing real-time efficient data anonymisation. In AEGIS it was utilized for offline, private usage. The use of a Blockchain-based IP and data sharing model and resulting micro-services for checking data quality, security, trust and IPRs and for enabling secure transactions had many advantages from an ethical perspective. They range from the difficulty of manipulation (due to its distributed nature), to the availability of self-governance transfer of ownership, able to capture the data value for each of the stakeholders involved (potentially including also the individuals' interest in taking advantage on their personal data). Another element with positive effects on privacy preservation was the selection of the repository for the storage depending on the applied disclosure and data privacy and IPR policy. Furthermore, AEGIS offers privacy-friendly and IPR-preserving modalities and tools for the extraction of linked data analytics from private harmonised data stored in private repositories or produced linked data with them resulting from the information exchange among ALLDS and the SLOD space.
Also in WP5 and its demonstrator-related activities, AEGIS partners paid attention to legal compliance towards the whole set of currently applicable legal instruments. The number of voluntary participants involved was limited at the strict necessary to test project solutions and, when possible, members of the research teams of the partners were engaged. The demonstrators used this AEGIS offline anonymisation tool (or/and similar anonymisation procedures): the AEGIS platform did not collect any personal data in the course of the project (and it has been conceived to operate in the same manner when concretely adopted in the market).

3.4.2. Demonstrator Case 1: Smart Automotive and Road Safety

The demonstrator case was not linked with self-driving car technology (usually termed autonomous driving). Thus, ethical problems of decision making by artificial intelligence did not arise. However, it was concerned with collecting data from vehicles operated in the field by volunteering drivers (who sign an informed consent). All (vehicle operation) data processed is anonymized.

One ethical issue could come up, if the information which would be delivered by the final product would be invalid and not reliable. If this is the case, is 1) an empirical question which cannot be addressed yet and 2) an ethical question: which degree of validity and reliability will be "sufficient" and will not raise ethical questions? These questions must be and can be discussed in course of time.

Data protection problems of the demonstrator case were of minor importance. Data to be collected during the experiments was sensor data (e.g. speed, acceleration, …) and/or simulation data. Sensor data was generated through connecting a device developed at VIF 'termed vehicle data logger' to the onboard diagnostic (OBD2) interface of a car. Simulation data was generated by study participants using a driving simulator developed at VIF and may include many additional values. Both sensor data and simulation data had to be stored on a

research server at VIF to allow the development of algorithms for inferring events including broken roads, patterns of safe and unsafe driving, or driving risks. Sensor and simulation data were kept on this server till the end of the project. Of course, all data was anonymized before being stored on the server.

The automotive and road safety demonstrator was located in Austria. The responsible national data protection authority in Austria is Austrian Data Protection Authority (in German: 'Datenschutzbehörde'), a governmental authority charged with data protection. The data protection authority is the Austrian supervisory authority for data protection, the equivalent of a national data protection commissioner in other countries.

The automotive and road safety demonstrator in the AEGIS project did not involve processing any personal data. However, there are two issues worth to mention.

(1) The geocodes of the starting points and the end points of car drives which were monitored and stored have the potential to de-anonymize drivers in low-density areas where in the extreme cases just one person lives on an area of one square mile or so. The solution of the project to deal with this data protection problem was clever: the data of the beginning and the end of a drive was not stored. In high-density areas one minute of data was not stored, in low-density areas this period is longer.

(2) According to the corresponding business scenarios and business models developed in the project and aiming to scale these applications to the market, a future collection of personal data might be considered. But at the end of the project there were no issues of data protection and ethics to be checked.

In the automotive demonstrator vehicle usage data was collected by 16 voluntary people employed at VIF, using a data logger developed at VIF connected to the OBD2 interface of their vehicle. Voluntary participants signed an informed consent and were well informed about the envisaged data collection process, the purpose of the data collection, the nature of the collected data, and use of the data within the AEGIS project.
Collected vehicle usage data was manually exported periodically from the data logger by a member of the AEGIS project team and then stored in an access-restricted AEGIS project folder located on a file share serviced by VIF's IT department. Exported data was anonymized and stored in folders like \\Projects\ AEGIS\Datasets \driver_id-01. Only the AEGIS project team had access to these folders.
The exported vehicle data collected was time series data and consisted of four comma-separated value (CSV) files per export to be stored into a folder.
Collected vehicle usage data was manually imported on the AEGIS Platform in the automotive demonstrator project in a dataset termed raw_data, using a similar folder structure (driver-id_vehicle-id_export-date) before executing the data processing pipeline to enable the three demonstrator applications (1) broken road indicator, (2) safe driving indicator and (3) regional driving risk estimator.

In order to make it even more difficult to manually identify a particular driver using GPS information, which was already virtually impossible, the start and the end of each time series were cut off.
All the voluntary participants were research staff of VIF: nevertheless, they were properly informed about all the details of data collection and processing, as well as and of the

conduction of the operations during the use cases before involving them and each of the volunteers signed the model consent form.
As a conclusion, after studying the details of the demonstrator, it is identified that suitable mechanisms were in place from the demonstrator partners, to deal with all ethical risks, including data protection.

3.4.3. Demonstrator Case 2: Smart Home and Assisted Living

The AEGIS SHAL demonstrator consortium partners followed a multi-fold approach towards safeguarding the privacy of the individuals participating in the SHAL demonstrator. More specifically the approach followed comprises of:
1. Physical separation of the database storing the sensitive, identifiable information of the individual, from the database holding the measurements retrieved from the smart watches and from the smart home environments. Towards this end, a physically separated database held the name, surname, e-mail address and IP address of the gateway of the smart home environment of the individual, along with the pseudonym of the individual, which comprised the unique identifier of the individual, with this pseudonym being used as the identification key in the second database holding the values of the various attributes measured. It should be noted that the SHAL consortium partners have opted for the pseudonymisation, rather than for the complete anonymization of the individuals, given the fact that the demonstrator aimed at providing personalised services (e.g. personalised alerts).
2. Processing of only the pseudonymized information. Within the context of the demonstrator, the information shared between the demonstrator backbone and the AEGIS platform was only the extract of the database holding the pseudonym of the individual, and the measurements of the various attributes. Towards this end, the only information that was processed on the AEGIS platform is the non-identifiable measurements associated with the individual's pseudonym, which was used for the re-classification of the individual into personas, and was then in turn returned back to the SHAL demonstrator backbone.
3. Encryption of the information. The physically separated database which held the name, surname, e-mail address and IP address of the gateway of the smart home environment of the individual, along with the pseudonym of the individual, was encrypted, so that even in the case an adversary gained access to it, the information contained in it was not disclosed.
4. Access Control. Access to both databases of the SHAL demonstrator backbone was restricted to the administrators of the backbone, and to the software developers of the three partners, using user names and passwords.
5. Accountability. All access attempts and actions within the context of the SHAL demonstrator were logged so that malicious actions could be tracked, traced, and not disputed.
Some additional clarifications pertaining specific types of data arriving from these devices were discussed and was clarified; geo-locational data was processed after acquisition to keep only the minimum necessary information (city, area) and not the exact latitude and longitude, biometrical information (height, weight) which represent sensitive data pursuant to article 9 GDPR was entered voluntarily and with explicit consent by the user, vital signs (blood pressure, heart rate) were recorded only for pre-specified purposes.
As a conclusion, all suitable mechanisms were put in place from the demonstrator partner, and all ethical risks were dealt in the final outcome.

The main purpose of the Smart Home and Assisted Living (SHAL) demonstrator was to illustrate and implement a services-bundle towards advanced holistic monitoring and assisted

living management, aiming to improve everyday living and enhance the wellbeing of people belonging to vulnerable groups.

The SHAL demonstrator implemented two main services, with respective scenarios, that can be offered by a care service provider to at-risk individuals and/or their (in)formal carers. In particular, the services were the following:

a) Services for monitoring and analysis of an individual's well-being conditions, physical activity, positioning and wearable information and external environment data (e.g. weather, crime, news, social media), towards the provision of a service for personalised notification and recommendation system for at-risk individuals, including notifications for carers.

b) Additional services pertaining monitoring and analysis of weather, indoor environmental conditions, energy and operational device data towards the provision of a smart home application, which can be offered by care providers to at-risk people for increased indoor comfort and welfare.

The data collected during the demonstration was used solely for the specific case (research activity) and completely destructed and removed from the AEGIS system after the case's finalisation. This fact is positive and neutral regarding ethical issues.

The number of the voluntary participants concretely involved was 12.

The data process lifecycle of the SHAL did not raised ethical issues because:

- Personal data was not stored locally and / or uploaded to the AEGIS platform during the Data Collection process.
- The collected data was not subjected to the appropriate offline pre-processing workflow and/or the anonymization process of deleting any sensitive element during the data preparation step.
- The datasets can be retrieved after their deletion during the storage step.

Some additional clarifications pertaining specific types of data arriving from these devices were discussed and clarified; geo-locational data was processed after acquisition to keep only the minimum necessary information (city, area) and not the exact latitude and longitude, biometrical information (height, weight) which represent sensitive data pursuant to article 9 GDPR was entered voluntarily and with explicit consent by the user (see declaration of consent), vital signs (blood pressure, heart rate) were recorded only for pre-specified purposes.

Regarding anonymisation, the AEGIS SHAL demonstrator consortium partners follow a multi-fold approach towards safeguarding the privacy of the individuals participating in the demonstrator.

As a conclusion, after studying the details of the demonstrator, it is identified that suitable mechanisms were put in place from the demonstrator partner, and all ethical risks were dealt in the final outcome.

3.4.4. Demonstrator Case 3: Smart Insurance

The AEGIS Insurance Demonstrator was aimed at exploiting the AEGIS platform Big Data technologies in order to access and analyse information coming from diverse and heterogeneous data sources, including the in-house data (e.g. customer location, insured/uninsured asset types), as well as weather, news and crime open data.

Using AEGIS solutions HDI data scientists are expected to be able to manage in an efficient way the occurring events (to happen or just happened), whilst the company is facilitated in setting-up a strategy to minimise the impact of the event on the company itself, and in offering support to the customers.

The demonstrator operations included the involvement of volunteers through the use of the developed Mobile App.

The voluntaries who participated during the development/testing phases of the project were 15 people (GFT or HDI employees). To test the second scenario (Personalized early warning systems for asset protection) 6 people from GFT/HDI were involved: they downloaded the Mobile App agreeing with the consent form provided. The other data was synthetic.
The partners involved in this demonstrator fine-tuned the project-level ethical, privacy and data protection overall strategy, with specific reference to both the Italian regulatory system and insurance sectors best practices and policies. They were aware and committed in complying with the ethics, privacy and data protection requirements.

The relevant data was those of the policies held by the customers and geo-location data provided by the HDI Mobile App, as well as the in-house datasets after anonymization.

The data used within the Insurance Demonstrator can be split in two main categories:

- External data, coming as open data from defined trusted websites.
  That kind of data refers mainly to events (e.g. weather, riots etc.) or to stats (e.g. flood risk distribution map, classification of seismic risk areas etc.).
- Internal data, named as in-house datasets, coming from the HDI databases.
  They are related to customers (e.g. customer data, policy data etc.) or to business data (e.g. agencies/agents, marketing data, claims data etc.).

The data used for the three scenarios execution named as in-house data was synthetic data that faithfully replies the data stored in the HDI databases.
Therefore, the Data minimization principle was pivotal, and attention was given to avoid collecting, processing or further processing personal data if not necessary. The amount of personal data which was gathered and used, was kept at a minimum amount.
Even if the data used for the analysis are synthetic, in order to simulate the reality as much as possible, the synthetic data has been anonymized for what concerns the personal data, making them not linkable with a person (in a real scenario). The anonymization has been made with the Anonymizer, the offline tool provided by a project partner and installed in a local HDI environment. The data was anonymised before their upload on the platform: only authorized

users can access them. In particular, HDI in-house datasets were anonymised through AEGIS Anonymisation tool: therefore, no personal data was managed and stored on the platform.

In the post project phase, it is envisaged that only the customers that have provided consent to the use of their data for analysis purpose, in particular in order to receive personalized offers, warnings and support for claims, will be able to use the AEGIS-based Mobile App. The in-house datasets are stored in the HDI servers. Only the data necessary for the analysis, after anonymization, will be filtered and uploaded on the platform by authorized users. This data is visible only to the HDI data scientists. At the end of the processing phase, the data scientist downloads the analysis output (it could be tabular, textual, graph) from the platform. Its use is managed by the data scientist within the HDI Systems (HDI Web App).

Also, purpose limitation principle, data storage limitation principle, data quality & accuracy principle, as well as confidentiality were addressed in the proper manner, whilst the use of automated processing was avoided: HDI operators will take decisions, though they will be supported by data analysis.

The insurance demonstration also underlines the potential benefit for the final user of AEGIS solutions: the customers will be provided with personalized services through the use of the AEGIS analytic tools, allowing to offer additional support and information about natural or social events of interest. The customer's satisfaction and positive feedback is expected to be improved. At the same time, all the customer's rights will be guaranteed.

Strict confidentiality policies and access restriction safeguards are taken by HDI in its daily data processing activity and were used in AEGIS demonstrator too, specifically customized for project purposes.

As a conclusion, the Insurance Sector Demonstrator considered and tackled in the proper manner the ethics, privacy and data protection strategy and related requirements. It included the implementation of all relevant ethics safeguards to ensure data protection and privacy and the respect of other ethics values. The amount of personal data to be collected to be able to provide the respective, personalized service was restricted to minimum necessary and the correct handling of data was conducted.

4. CONCLUSION

This Ethics White Paper (EWP), capitalizing on AEGIS project's experience, is aimed at offering a focused and practical guidance and best practices for dealing with ethical issues in Big Data Horizon 2020 projects, proposing ways of progressing the action and developing research results in a constructive and ethically-compliant manner. The document provides a set of best practices and lessons learnt on how reflecting ethics considerations in project activities and results, seeking to adequately tackle with the legal and ethical issues and concerns at stake and, among other, to ensure responsible and accountable use of personal data.

It offers suggestions and tips for getting project development and outcomes 'ethics-compliant' under Horizon 2020 and the applicable regulatory framework (international, EU and national law). It may be considered as an example of tools for operationalizing responsible research and innovation principles, H2020 ethical guidelines and data ethics in the framework of research projects, by mitigating some of the main risks, in terms of the privacy and ethical challenges associated with Big Data's use.

Nevertheless, it is not intended to replace ethical reasoning for the identification of the relevant ethical issues, as well as for the elaboration and application of proper countermeasures on a case-by-case basis, if opportune with the support of specialised ethics experts.

This is a living document. For further contributions, please contact the main author:

Marina Da Bormida
R&I Specialised Lawyer and Ethics Expert
m.dabormida@eurolawyer.it
+393498433690