
**PROJECT DELIVERABLE REPORT**


# Introducing advanced ICT and Mass Evacuation Vessel design to ship evacuation and rescue systems

## D1.7 Ethics State-of-the-Art Report

A holistic passenger ship evacuation and rescue ecosystem

MG-2-2-2018

Marine Accident Response

*"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814962"*

## Document Information

| Grant Agreement Number | 814962 | Acronym | PALAEMON |
|---|---|---|---|
| **Full Title** | A holistic passenger ship evacuation and rescue ecosystem | | |
| **Topic** | MG-2-2-2018: Marine Accident Response | | |
| **Funding scheme** | RIA - Research and Innovation action | | |
| **Start Date** | 1st JUNE 2019 | **Duration** | 36 months |
| **Project URL** | www.palaemonproject.eu | | |
| **Project Coordinator** | AIRBUS DEFENCE AND SPACE SAS | | |
| **Deliverable** | D1.7 Ethics State-of-the-Art Report | | |
| **Work Package** | WP1 – Project Management, Quality Assurance and Reporting | | |
| **Date of Delivery** | **Contractual** M9 | **Actual** | M10 |
| **Nature** | R - Report | **Dissemination Level** | PU-PUBLIC |
| **Lead Beneficiary** | JOAFG | | |
| **Responsible Author** | Georg Aumayr<br>Gudrun Ringler | Email | Georg.aumayr@johanniter.at; Gudrun.ringler@johanniter.at |
| | | Phone | +43 1 470 70 30 3033 |
| **Reviewer(s):** | Eberhard Koch, Philippe Chrobocinski | | |
| **Keywords** | Ethic, GDPR, EESSR, assessment, state of the art (SOTA) | | |

## Revision History

| Version | Date | Responsible | Description/Remarks/Reason for changes |
|---|---|---|---|
| 0.1 | 2020/02/04 | Georg Aumayr, Gudrun Ringler | Report write-up |
| 0.2 | 2020/02/18 | Gudrun Ringler | Inclusion of partners' contributions |
| 0.3 | 2020/02/26-2020/03/09 | Eberhard Koch, Philippe Chrobocinski | Internal Review |
| 1.0 | 2020/03/11 | Gudrun Ringler | Review and Release |

## Contents

## Abbreviations

| | |
|---|---|
| AAL | Active and Assisted Living |
| ALLEA | All European Academies |
| CA | Consortium Agreement |
| DESCA | Development of a Simplified Consortium Agreement |
| EESSR | Ethic Evaluation Standard for Security Research |
| GDPR | General Data Protection Regulation |
| IMO | International Maritime Organization |
| MEESTAR | Model for the Ethical Evaluation of Socio-Technical Arrangements |
| MEV | Mass Evacuation Vessel |
| The Charter | The Charter of Fundamental Rights of the EU |
| UAV | Unmanned Aerial Vehicle |
| WMA | World Medical Association |

# 1 Executive Summary

In this deliverable, ethical and legal aspects in regard of the project PALAEMON are presented. The Charter of Fundamental Rights serves as guideline for human interacting in our social cultures and therefore leads to ethical principles and their bundles, described in chapter 5 State of The Art in Ethics for PALAEMON. Furthermore, as social research with participant involvement will be conducted, and this of course needs a special monitoring not to harm anyone's rights in regard of his/ her data sovereignty, the General Data Protection Regulation of the European Union is an important part in this deliverable. However, it must be taken into account that only the most important paragraphs (for the project) are worked on and explained in regard of PALAEMON's context.

Furthermore, EESSR, an ethical evaluation model, that supports the identification of ethical dilemmas in the process of technical developments for the safety and security sector, is described. It is planned to apply this tool in regular workshops during the whole project duration (more in D1.8).

## 2 Introduction

Ethic is a large term that covers different dimensions of moral, cultural aspects and legal aspects. In general, ethics is about “how to live a good life”. What ethic is about, was discussed for centuries by Platon, Aristoteles, Thomas of Aquino, René Descartes, Immanuel Kant, G W.F. Hegel, Friedrich Nietzsche, Jean-Paul Sartre and many more.

The big consensus is that there is a moral that is necessary for living together and that is the foundation of what we call legislation. Jurisdiction is applied ethics.

In research, ethics has a special position. Already in the 17th and 18th century, medical doctors were by moral standards not allowed to excavate and dissect human bodies. Despite of this, some doctors started to do this to learn more about anatomy. This was the first rush of science to boost medical approaches. The tension between moral standards in a cultural environment and the possibilities of science and technology are providing the dynamic of applied ethics in this field. At this time, the discussion about genetic modification has a similar impact on medical standards as the start of dissection was.

For PALAEMON, the question of saving lives with new forms of lifeboats is at first sight very easy.

But the discussion about environment pollution, unnecessary travels, waste and plastic in the sea etc. is offering a huge field of discussions.

Is it applicable to use commercial standards for lifesaving measures?

If everyone needs to be saved, who should be first and who should be last?

What is an acceptable loss of a ship or crew or passengers?

How should people be treated after the lifesaving action?

How long do you have to search for missing people?

Next to these very principle questions, there are questions about PALAEMON’s technology itself which are important, as they are potentially touching moral issues like privacy, self-perception and personal security.

Are the wristbands for detection just used during an evacuation procedure?

What is the use of Unmanned Aerial Vehicles (UAVs) data in the decision making process?

Would an automated mustering system be a real support and stable enough that the crew may rely on it?

What is safety worth for the development of the Mass Evacuation Vessels (MEVs)?

What is the main purpose of the MEVs? Commercial use as functional spaces during the voyage (e.g. passenger cabins) or just for evacuation?

There are legal aspects related to these questions, mainly concerning the General Data Protection Regulation. But there is a certain tension between international waters and EU legislation, which has to be applied for the reason of an EU funded project. Also the situation

of the usage is demanding different perspectives. Under the condition of a disembarkment procedure, rules for crisis management (in regard of free access to all data by first responders) changed and provide certain freedom of actions concerning data protection and privacy.

We want to state following principles for the general approach:

1. Safety first!
   Seafarers' safety is prior to all actions on the boat. If a trained seafarer fails or get wounded, the disembarkment action is threatened. A wounded sailor is not supporting others.
2. Life goes before injury
   Time is lifesaving. If a comfortable or a fast support is optional, go for the fast option. If there is a threat of injuries for a passenger, it has to be taken into account for saving as many lives as possible.
3. Equality of passengers
   Independent of the booking status of the passengers, all have to be dealt with in the same way.

# 3 Legal Aspects

Within the PALAEMON project social research, technologic developments but also the ultimate goal of lifesaving targeted by the project need a proper look at the legislation in charge. Laws serve as binding guidelines of ethically correct acting in our cultures as they are the expression of our moral sense.

## 3.1 Charter of Fundamental Rights

The Charter of Fundamental Rights of the European Union (hereinafter 'the Charter') brings together in a single document the fundamental rights protected in the EU. The Charter contains rights and freedoms under six titles: dignity, freedoms, equality, solidarity, citizens' rights and justice (The Council of the European Union, 2013). The Charter became legally binding in 2009 when it was signed together with the Treaty of Lisbon. This means that all European legislation needs to conform to the principles of the charter, including research policies. Several principles of the Charter are relevant in the context of research policy and the aim of the project – they are depicted below.

*Article 3 - Right to the integrity of the person (dignity)*

1. 'Everyone has the right to respect for his or her physical and mental integrity'.

2. 'In the fields of medicine and biology, the following must be respected in particular: the free and informed consent of the person concerned, according to the procedures laid down by law'.

*Article 8 - Protection of personal data (freedoms)*

1. 'Everyone has the right to the protection of personal data concerning him or her'.

2. 'Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.'

3. 'Compliance with these rules shall be subject to control by an independent authority'.

*Article 21 - Non-discrimination (equality)*

1. 'Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.'

*Article 24 - The rights of the child (equality)*

*2. 'In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.'*

*Article 25 - The rights of the elderly (equality)*

'The Union recognizes and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life.'

*Article 26 - Integration of persons with disabilities (equality)*

'The Union recognises and respects the right of persons with disabilities to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community.'

*Article 38 – Consumer protection (solidarity)*

'Union policies shall ensure a high level of consumer protection'.

### 3.2 GDPR

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter 'GDPR' or 'Regulation') (The European Parliament and the Council of the European Union, 2016) entered into force in May 2016.

'The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.' (GDPR.EU)

As regulation it is directly to be set in place and is applicable for PALAEMON.

First, as it is all about personal data, the definition by the European Commission (European Commission, n.d.) is presented:

Article 4 (1) ''Personal data' means 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 more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' (GDPR.EU)

The EC names following examples for personal data:

- 'a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;

* *Note that in some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies – the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1).'* (European Commission, n.d.)
The ePrivacy Directive (The European Parliament and the Council of the European Union, 2002) is not applicable for PALAEMON as location data are defined by the EU as follows:
Art. (2c) 'location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;'

- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

(European Commission, n.d.)

Further, the European Commission clearly describes how data are allowed to be processed, following the GDPR:

'Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the GDPR.

Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

The GDPR protects personal data **regardless of the technology used for processing that data** – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.' (European Commission, n.d.)

### 3.2.1 The GDPR and PALAEMON

From the beginning on, the GDPR makes clear that data processing of data of identifiable natural persons is forbidden - the exceptions are also stated in the regulation. In PALAEMON with data will be dealt within the conducted scientific research but also by the scope of the project and its solution for a safer shipping.

In (26) is stated:

' …To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. …' Following, measures must be taken, when field trials will be conducted in WP8 but also in other applied methodologies of social research in the case persons are involved and data generated/ stored/ processed. Furthermore, as PALAEMON deals with technology that take up and transmit data (e.g. tracking wristbands and/ or drones), this paragraph has to be given consideration.

However, associated to the work of PALAEMON and especially the social research in the project are also the paragraphs

- (33) concerning research data,
- (40) as determination of how to make data processing legal,
- (42) for informed consents,
- (59) concerning erasure of personal data,
- (60) concerning transparency,

Further, concerning the issue with handing over personal data from automated means, this paragraph (68) allows the participants of a research project to receive their own data and to ask for the handover to another controller. This paragraph needs to be kept in mind as it is foreseen that in PALAEMON wristbands and drones will be used for delivering location-data of the participants.

Furthermore, in (71) is stated, that individuals have the right not to be subject to a decision that could have also a significant effect on his/ her, based solely on personal data of automated processing without any human intervention. These personal data also include location or movement data, which shall be used in our project. In PALAEMON it is foreseen that these data are processed automatically or semi-automatically, but the ultimate decision about e.g. evacuation routes is in the hand of the Master. By this, at this point of time no restriction in regard of this paragraph is seen for the project.

In (78) it is stated that a structure has to be provided to ensure the safeguard of data protection and the chance for people to ask for their rights. Appropriate technical and organisational measures have to be taken to ensure that the requirements of this regulation are met. This makes the legal framework necessary to understand and develop with these requirements in mind.

Such measures could consist, inter alia, of minimising the processing of personal data, anonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

It is very clearly stated that the regulation is also valid for development processes.

For the project and its evaluation and developments, it is necessary to have an inventory of data processing as well. In (82) it is requested to have an inventory of data processes and data usage for demonstrating compliance to the GDPR.

Furthermore, for the project and its developments, it is necessary to have a data protection impact analysis:

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing. In (92) it is implicit mentioned that this is considered for projects (of a general type, including PALAEMON) as well.

In case of a violation of data protection, the data subject has to be informed as soon as the responsible party becomes aware of the violation (see (86)).

Paragraph (98) declares that associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct to facilitate the effective application of the GDPR. In PALAEMON we need to think about bodies (e.g. shipping companies, coast guard services, IMO, flag states, SAR centers) who could be responsible in future in the sense of its implementation.

For PALAEMON it also must be thought of data transmissions to (international) bodies in third countries. Transfers to third countries which provides an adequate level of protection (approved by the EU), may take place without the need to obtain any further authorization. (103) Further, as it is stated in (108), in the case of absence of such an EU-approval, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject.

Further, the transmission of personal data to third parties is allowed when life is endangered. This includes the life of the data subject but also third people or the general public: '… A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. …' (112)

The paragraphs (159) and (162) are important for scientific research:

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Paragraph 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

### 3.2.2 Principles as guidelines for development

In Chapter II, Article 5 (1) the principles of data protection are stated as

(a) Lawfulness, fairness and transparency

processed lawfully, fairly and in a transparent manner in relation to the data subject

(b) Purpose limitation

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

(c) Data minimization

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

(d) Accuracy

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

(e) Storage limitation

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

(f) Integrity and confidentiality

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

(g) Accountability by the controller

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1

This provides something like a general guidance through data protection for technologic developments. Especially 5(1)c is interesting for projects like PALAEMON. As data may be just processed and used in a predefined way, data mining is in question if not stated in an informed consent as a dedicated aim.

The processing of data and use of personal data is just allowed when at least one of the following points are met according to Article 6 (1):

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

For PALAEMON, this requirement can be fulfilled with an Informed Consent that need to be signed by individuals participating for social research matters. Further, for implementing PALAEMON-developments in future shipping, it needs to be thought of Informed Consents for signing by each passenger as part of the cruise booking procedure, for example.

Art 7 (1) declares that the controller shall be able to demonstrate that the data subject has consented to processing his/her data. Therefore, it is necessary to pay attention and to proof that an informed consent has been by each subject.

Further, the participants have at any time the right to withdraw from the project (Art 7(3)).

### 3.2.3 Informed consent

Chapter III concerns the rights of affected persons. Section 1 and 2 are focused on transparency of information and access to personal data.

In Art 12 in Section 1 is declared, that information relating to data processing and given to the data subject must be 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language', provided in a written and if requested in an oral form.

Further, if requested by the data subject, the controller must give information on the action taken in due time (1-3 months). Otherwise the controller is in need to give reasons.

The headline 'Information to be provided where personal data are collected from the data subject' of Art 13 in Section 2 reflects perfectly its programme. As this section is very important, the original regulation text is presented here:

(1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

> (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
>
> (b) the contact details of the data protection officer, where applicable;
>
> (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
>
> (d) where the processing is based on point
>
> (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
>
> (e) the recipients or categories of recipients of the personal data, if any;
>
> (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49 (1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

> (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

(4) Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Further, in the case personal data have not be obtained by the data subject – in PALAEMON this could be e.g. location data – the controller must give information about

- identity and contact details of the controller,
- contact details of the data protection officer
- the purposes of the processing and its legal basis
- the categories of personal data concerned
- the recipients of the personal data

to the data subject. (Art 14 (1)).

In paragraph (2) the information is listed that must be given to the data subject ‘to ensure fair and transparent processing in respect of the data subject’ (e.g. period of data storage, existence of rights of data subjects, existence of automated decision-making).

In Art 15 the ‘Right of access by the data subject’ is regulated, mainly which data it concerns.

### 3.2.4 Rectification and erasure

Something new in data protection is the right of rectification and erasure, regulated now in the GDPR. Especially the right for erasure is in this form something new to be stated. Both are presented in Section 3:

Art 16, Right to rectification, ‘The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.’

Art 17, Right to erasure (‘right to be forgotten’),

(1) 'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6 (1), or point (a) of Article 9 (2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21 (1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21 (2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8 (1).'

For PALAEMON and shipping in general, following Art 17 (1a) the point of time of erasure could be the normal disembarkation/ the end of the booked cruise.

(2) 'Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.'

(3) 'Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.'

In Art 17 (3d) the right of erasure of data for scientific sets, is excluded. This allows some degrees of freedom and feasibility for PALAEMON as a research project. Nevertheless, after the project has ended, data has to be erased.

### 3.2.5 Portability and interoperability

In the GDPR Article 20 states the right to data portability. This means that personal data can be transferred from System A to System B or System C by the data subject. The controller of System A – in this example – has to provide the requested data 'in a structured, commonly used and machine-readable format' and thus in an exchangeable way to the data subject but

also directly to another controller if the data subject claimed it. By this, interoperability is of importance concerning the legal situation and the rights of persons whose data is gathered of.

It is the responsibility of development to ensure that data can be transferred between parties or systems.

### 3.2.6 Objection

Article 21 regulates the right to object. Paragraph (6) names exceptions – besides others- scientific research, argued with the public interest.

### 3.2.7 Automated individual decision-making

In PALAEMON early risk detection and adjusted interventions are major issues. Ideally, this can be done in an automated way by certain algorithms. In the GDPR this is addressed in Article 22: in general, the data subject has the right not to be part of an automated analysis procedure (including profiling). Paragraph 2 provides in (a) and (c) ways for allowance in terms of PALAEMON.

### 3.2.8 Technical requirements by law

The technical requirements given by law are stated in a way that puts the usage before technology and defines by this action and obligations, not exact technologies.

It is stated in Chapter IV, Article 24 what the responsibilities of the controller are. In general, the controller has to take care that the data subject can make use of all his or her rights. In paragraph (1) this is made clear:

Art 24 (1) ‘Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.’

To ensure these obligations, a certification process and code of conduct are referred to in article 40 and 42. Both are available here in this document under 3.2.15 Code of Conduct.

Further, also Article 25 is relevant in this context: in the title is stated that data protection is already a design but also a default issue.

Article 25, ‘Data protection by design and by default,

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In

particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(3) An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

### 3.2.9 Joint controllers

Also in Chapter IV the joint controllers are discussed and regulated (Article 26). In the case, in PALAEMON has two or more controllers, they are named as joint controllers. Joint controllers have the same duties as controllers, but furthermore, '… by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.'

### 3.2.10 Processors

Article 28 of chapter IV of the GDPR describes an important role: the processor. Following the whole article is presented:

Art. 28, 'Processor

(1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

(2) The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(3) Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

> (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
>
> (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
>
> (c) takes all measures required pursuant to Article 32;
>
> (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
>
> (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the

fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

(4) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

(5) Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

(6) Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

(7) The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

(8) A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

(9) The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

(10) Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

### 3.2.11 Inventory of processing activities

For transparency, it is required to keep record of processing activities. How this is done and which formal criteria have to be met is stated in Article 30:

Art 30, Records of processing activities,

(1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

> (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
>
> (b) the purposes of the processing;
>
> (c) a description of the categories of data subjects and of the categories of personal data;
>
> (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
>
> (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
>
> (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

(2) Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

> (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
>
> (b) the categories of processing carried out on behalf of each controller;
>
> (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
>
> (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

(3) The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

(4) The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

(5) The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

### 3.2.12 Security Standards

In Article 32 (1) security standards are mentioned. Technical and organizational measures have to be appropriate and state of the art and in relation to the scope, context and purpose of the processing that is done.

> (a) 'the pseudonymisation and encryption of personal data;
>
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
>
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'

In paragraph (2) the assessing of security level and risk analysis is mentioned:

(2) 'In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.'

This will be necessary for developments throughout the project.

Further, in this article:

(3) Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

(4) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

As paragraph 2 in article 32 declares the risk analysis, it is even more explicit in article 35 Data protection assessment and prior consultation.

This article 35 is of importance to PALAEMON, because it is stating in its first paragraph already the development of new technology. Also in paragraph 7 the basic requirements for the risk analysis or data protection impact assessment are formulated:

Article 35, Data protection impact assessment

(1) '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. A single assessment may address a set of similar processing operations that present similar high risks.

(2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

(3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

(4) The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

(5) The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

(6) Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(7) The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

(8) Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

(9) Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(10) Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the

context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

(11) Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.'

### 3.2.13 Prior consultancy

In article 36 (1) the controller shall consult a supervisory authority prior to processing personal data, when a data protection issue according to article 35 is given. By paragraph (3), the basic needed information is listed:

(3) 'When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

> (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
>
> (b) the purposes and means of the intended processing;
>
> (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
>
> (d) where applicable, the contact details of the data protection officer; 4.5.2016 L 119/54 Official Journal of the European Union EN (e) the data protection impact assessment provided for in Article 35; and (f) any other information requested by the supervisory authority.

### 3.2.14 Data protection officer

The data protection officer is requested by article 37(1c):

(1) 'The controller and the processor shall designate a data protection officer in any case where:

> (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
>
> (b) 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
>
> (c) 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.'

For PALAEMON this can be one assigned person, as the project can be considered as a group of undertaking. Therefor - following 37 (2) - one data protection officer is sufficient:

Art 37 (2) 'A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.'

The data protection officer has to fulfil a certain profile by 37 (5):

Art 37 (5) ‘The data protection officer 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.’

As article 39 is mentioned, a short excurse to this is needed to summarize the qualification profile. This article 39 states the scope and tasks of the data protection officer:

Article 39, Tasks of the data protection officer

(1) ‘The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

(2) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.’

The data protection officer has to be named by the controller publicly (see Art 37(7)). For PALAEMON this can be done on the official project website (https://palaemonproject.eu/). This announcement has to have the full contact data of the data protection officer. Also this information has to be given to the data protection authority. In the case of PALAEMON, this could be a gremial of the EC.

Within a controller and/or processor, the data protection officer has a special position. This position is declared in Article 38:

Article 38, Position of the data protection officer

(1) The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

(4) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

(5) The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

(6) The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

### 3.2.15 Code of Conduct

The Code of Conduct and its certification (Section 5 of the GDPR) has to be part of the development process and helps in shaping the data structure. For this, it is stated here in after.

Article 40, Codes of conduct

(1) 'The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

(2) Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

(3) In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall

make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

(4) A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

(5) Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

(6) Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

(7) Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

(8) Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

(9) The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

(10) The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

(11) The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 42, Certification

(1) The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

(2) In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate

safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

(3) The certification shall be voluntary and available via a process that is transparent.

(4) A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

(5) A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

(6) The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

(7) Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

(8) The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

### 3.2.16 Transfers

In Chapter V ‘Transfers of personal data to third countries or international organisations’ are regulated.

The general principle (Article 44) says:

‘Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. … .’

To sum it up, the European Commission must certify the third country or the international organisation in regard of an adequate data protection and must monitor developments of them that could affect the data protection.

However, in Art (46) is declared that – in the case this certification is missing – personal data are allowed to be transferred, ‘if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies

for data subjects are available.' Following the necessary conditions are formulated in the GDPR.

In the today's practice, passengers' personal data, the passports, residences as well as credit card-data are taken at the check-in. Additionally a photo of each passenger is taken and placed on his embarkation card, to be shown at any port, before leaving and entering the passenger ship. All personal data are transferred to immigration authorities, customs etc. at any port called - even in third countries.

However, in PALAEMON but especially when implementing the project's results and developments into real life, this chapter could be important as data might need to be transferred additionally to e.g. an international organisation.

### 3.2.17 Supervisory authorities

Chapter VI of the GDPR is all about the national supervisory authorities that must work independently, e.g.: conditions, tasks, competences and powers.

These institutes should be contacted in any case of ethical doubts and questions of understanding or interpretation concerning the GDPR. Further, the supervisory authorities give advice, monitor and cooperate with other supervisory authorities from other countries.

However, in the context of the PALAEMON project it must be taken into account too, that in international waters international regulations may not apply or may apply in a restricted way.

# 4 Ethics in the Project's Contracts

The following section represents regulations in the ethical context described in contracts of the project, the Grant Agreement and the Consortium Agreement.

## 4.1 Grant Agreement

Ethics in regard of PALAEMON – as a Horizon 2020 project - are asked for by the EC and proposed by the consortium in Section 5.1 of the submitted proposal version that serves also as basis for the Grant Agreement.

### 4.1.1 Proposal

Following is written in the proposal:

'At its core the PALAEMON project will collect and analyse large volumes of data coming from different sources. While a big portion of these data will originate from public sources, PALAEMON may also process proprietary or confidential data such as financial reports and market analyses. To this end, a dedicated task is specified in PALAEMON's work plan. Within its scope, a detailed data management plan (D1.4) will be devised ethics (D1.8) that will be revised according to any ethical issues that will have to be addressed during the project's lifecycle.' (Consortium of PALAEMON, 2018)

Further, the consortium commits to work in line with ALLEA' European Code of Conduct (see 5.2) as well as with the Responsible Research and Innovation Principles of the EC which central premise is to work together. This doesn't only include researchers but also citizens, policy makers, business and so on. The aim is to support the process but also to receive holistic outcomes including values, needs and expectations of society. (European Commission, n.d.)

Additionally, the consortium's aim in regard of working with participants in the ethical context is to preserve the mutual respect and confidence. Therefore, the consortium will push the principle of information and – especially in the recruitment phase – the principle of prior, free, unambiguous and informed consent. The research will be carried out with the focus on not to disturb the participants' health, dignity and well-being in accordance with non-discrimination and non-malevolence.

In regard of collected data the consortium commits explicitly to ensure the protection of personal data and – of course – to comply with the GDPR (see 3.2.1) and national data protection regulations, fundamental rights, directives and opinions embedded in the regulatory framework of the EU.

Therefore, besides of others, a data controller will be established. Further: 'As the whole project will strictly follow the ISO 27001 (for information security management) recommendations, it will be in line with the corresponding information classification policy of each Industrial sector and will handle the corresponding information accordingly.' (Consortium of PALAEMON, 2018)

### 4.1.2 Grant Agreement

However, in the Grant Agreement of PALAEMON (EC Innovation and Networks Executive Agency, 2019) in chapter 4, section 4 ethical issues are taken into account:

The first paragraph concerns the researchers; in particular their recruitment and working conditions (Art. 32).

In Art. 33 gender equality is promoted.

Article 34 declares ethics and research integrity: the consortium must carry out the action in compliance with ethical principles and applicable international, EU and national law. Further it is explicitly mentioned that the consortium must respect the fundamental principles of research integrity and has to take the actions in compliance with reliability, honesty, respect and accountability (Art. 34.1).

Art. 34.2.: 'Before the beginning of an activity raising an ethical issue, each beneficiary must have obtained:

(a) any ethics committee opinion required under national law and

(b) any notification or authorisation for activities raising ethical issues required under national and/or European law

needed for implementing the action tasks in question.'

In Art. 35.1 it is declared that conflicts of interests have to be avoided.

The consortium is obliged to keep each information, data, documents and other material confidential for four years– if not requested and agreed on for a longer period. But, the Agency has the right to disclose confidential information to its staff, other EU institutions and bodies if it is necessary to implement the Agreement or to safeguard the EU's financial interests.

### 4.2 Consortium Agreement

The Consortium Agreement (CA) (DESCA, adapted by the Consortium of PALAEMON, 2019) regulates the collaboration of project partners and therefore represents a kind of code of conduct.

Especially two sections are important in regard of ethics:

- Sect. 5: Liability towards each other
- Sect. 11: Personal Data Protection

In Section 5 the liability towards each other – as the title already suggests – is described:

The represented rules follow the Belgian law governing liability and shall apply to each claim between the parties for loss or damage caused by another party.

First, the giving party gives nor warranty to the receiving party in regard of materials and information, its sufficiency or property rights (of third parties). Therefore, the receiving party is solely liable for the use (5.1) and also for any loss, damage or injury of third parties (5.3).

In 5.2 limitations of the liability are regulated. A party that caused damage or loss is not liable in following cases, even not if '… such Party was informed or aware of the possibility thereof:

- Loss of profits, revenue, income, interest, savings, shelf-space, production and business opportunities;
- Lost contracts, goodwill, and anticipated savings;
- Loss of or damage to repetition or to data;
- Costs of recall of products; or

- Any type of indirect, incidental, punitive, special or consequential loss or damage

The foregoing exclusion shall not apply in the case of any breach by a Party of its obligations under Section 10 (Non-disclosure of Confidential Information). (DESCA, adapted by the Consortium of PALAEMON, 2019)

For each party the financial liability is limited for all claims of all parties by the total costs of the project defined in the Grant Agreement (Annex 2), if the damage was not caused wilfully, fraudulently or by gross negligence.

The exclusions above and the financial limitations are not valid in the case of infringement of the IPRs. Further, in 5.2.5 other exceptions are named, all based on wilfulness, e.g.: fraud, death, injury to natural persons or damage to real or immovable property.

‘5.4 Force Majeure

No Party shall be considered to be in breach of this CA if it is prevented from fulfilling its obligations under the CA by Force Majeure. …’ (DESCA, adapted by the Consortium of PALAEMON, 2019)

In Section 11 the Personal Data Protection that refer to the GDPR, is described in the framework of the collaboration of project partners. It says, that each party is in charge of the processing of personal data by itself and is responsible to apply appropriate technical and organisational security measures. This is also valid if the party processes personal data on behalf another party. Further, in the CA is fixed, that the partners must sign an agreement regarding processing of personal data through which they establish principles of their activities in this regard; latest at the point of time of the first disclosure of personal data.

# 5 State of The Art in Ethics for PALAEMON

Ethical aspects are a determining facet of our societal mindsets and action. Thus, also our professional lives and collaborations and by these professional actions are guided by them. For reflection and a common understanding of the society ethics are dealt with in Codes of Conduct or Code of Practice and its principles (that are naturally in line with the legal requirements). Following some of these guidelines that also relate to the project PALAEMON and its work are introduced to the reader.

## 5.1 RESPECT Code of Practice

For European scientific work in the socio-economic environment and information technologies, the RESPECT Code of Practice is used in several studies.

Within the RESPECT Code of Practice existing Codes of Conduct are merged and connected to the EU-legislation. However, the RESPECT Code of Practice is based on three main principles that should also be the main pillars of each Code of Conduct for the application of socio-economic research:

- Upholding scientific standards (e.g.: citation, objectivity)
- Compliance with the law (especially data protection law and intellectual property law)
- Avoidance of social and personal harm

The RESPECT Code of Practice's use is voluntarily. Moreover, it can be interpreted as suggestion and basis for further Codes of Conduct that could also need a refinement for tailor-made principles and therefore individualisation.

Its application can be seen as support and shall foster an informed decision-making.

(RESPECT project, 2004)

## 5.2 ALLEA European Code of Conduct for Research Integrity

'The European Code of Conduct for Research Integrity serves the European research community as a framework for self-regulation across all scientific and scholarly disciplines and for all research settings.

The 2017 revised edition of the Code addresses emerging challenges emanating from technological developments, open science, citizen science and social media, among other areas. The European Commission recognises the Code as the reference document for research integrity for all EU-funded research projects and as a model for organisations and researchers across Europe.' (All European Academies, 2017)

In the All European Academies' (ALLEA) European Code of Conduct for Research Integrity (All European Academies, 2017) 4 fundamental principles of research integrity are declared for guiding researchers in their work:

- Reliability
- Honesty
- Respect
- Accountability

Following are good research practices in the contexts of

- Research Environment
- Training, Supervision and Mentoring
- Research Procedures
- Safeguards
- Data Practices and Management
- Collaborative Working
- Publication and Dissemination
- Reviewing, Evaluating and Editing

described and the research misconduct (fabrication, falsification, plagiarism) and other unacceptable practices (e.g. manipulating authorship, withholding results, allowing funders/sponsors to jeopardise independence) defined.

### 5.3 Standards of Conduct for the International Civil Service

The UN Ethics Office is providing a Standard of Conduct for the International Civil Service. By this the standards are intended as a behavioural and ethical guide for international civil servants, for whom competence, integrity, impartiality, independence and discretion are taken as granted, but furthermore, who have to serve the ideals of peace, respect for fundamental rights, economic and social progress as well as international cooperation. These values are reflected in 49 principles – splitted in the topics

- Guiding principles
- Working relations
- Harassment and abuse of authority
- Conflict of interest
- Disclosure of information
- Use of the resources of United Nations organizations
- Post-employment restrictions
- Role of the secretariats (headquarters and field duty stations)
- Staff-management relations
- Relations with member States and legislative bodies
- Relations with the public
- Relations with the media
- Use and protection of information
- Respect for different customs and culture
- Security and safety
- Personal conduct
- Outside employment and activities
- Gifts, honours and remuneration from outside sources

The International Civil Service Commission recommends organizations of the United Nations system to overtake the Standards of Conduct, but expects to preserve the independence and impartiality of the international civil service.

(International Civil Service Commission, 2013)

### 5.4 Code of Ethics for IMO Staff members

As a specialized agency of the United Nations, the International Maritime Organization (IMO) is the global standard-setting authority for the safety, security and environmental performance of international shipping. Its main role is to create a regulatory framework for the shipping industry that is fair and effective, universally adopted and universally implemented. (International Maritime Organization, n.d.)

The IMO's Code of Ethics, which is based on the United Nation Ethics Committee's model Code of Ethics text – as the IMO declares - , was developed to secure standards of efficiency, competence and integrity and shall serve as a guidance document for understanding the ethical standards and conduct required of all employees in the performance of their duties. Furthermore, IMO's Code of Ethics is also applicable for staff members of entities and individuals who entered a cooperative arrangement with IMO.

The present Code of Ethics consists of 6 values:

1. Independence (as IMO is an independent organisation)
2. Loyalty
3. Impartiality (impartiality, objectivity and professionalism)
4. Integrity (including honesty, truthfulness, fairness and incorruptibility)
5. Accountability
6. Respect for human rights (act with understanding, tolerance, sensitivity, respect for diversity and without discrimination)

and following 6 principles:

1. Conflict of interest
2. Abuse of authority
3. Gifts, honours, favours or other benefits
4. International Maritime Organization resources
5. Confidentiality of information
6. Post-employment.

(International Maritime Organization, 2016)

### 5.5 Helsinki Declaration

The World Medical Association (WMA) Declaration of Helsinki (World Medical Association, 2018) is developed for the field of medical research – as the subtitle reveals. The declaration is one of the most common papers that describes shortly ethical principles on an international level and is almost always used as (part of) ethical guidelines in medical studies.

Abstaining from the medical topic, a bundle of mentioned ethical aspects are very similar and also relevant for social research as human beings are involved as researchers and as participants.

Following ethical aspects of the declaration can be transferred to social research (World Health Organisation, 2001):

- The ethical principles provide guidance to the researcher and the participants.

- The ethical standards should promote respect for human beings and protect their health and rights.
- Researchers should protect life, health, privacy and dignity of the participants.
- The researcher shall act only in the participant's interest.
- The well-being of the participant should take precedence over the interests of science and society.
- The participants must be volunteers and adequately informed, especially about potential risks, anticipated benefits and possible conflicts of interest.
- The participant's integrity must be respected.
- The privacy of the participant must be respected.
- Patient's information and data must be handled confidentially.
- Participants must be informed to have the right to withdraw from the participation on the study or to withdraw at any time without reprisal. After ensuring that the participant understood the information the researcher should obtain the freely-given informed consent, preferable in writing.
- Vulnerable populations require special protection. In the case the participant is legally incompetent, physically or mentally incapable of giving consent or is a legally incompetent minor, the legally authorized representative needs to be involved and give the informed consent (with accordance to the applicable law).
- Research with persons' involvement needs to take generally accepted scientific principles of science into account and should be performed only be scientifically qualified persons.
- Researchers should abstain from engaging in research involving persons unless they are confident with the risks that are adequately assessed and can be satisfactorily managed.
- The design of research with participants' involvement should be clearly formulated and documented. The document must be reviewed in regard to ethical aspects.
- Authors and publishers have ethical obligations. Researchers are obliged to preserve the accuracy of the results; negative as well as positive results should be published.
- The ethical board/ reviewer should be in conformity with laws and regulations of the country in which the social research is performed.

How all these requirements could be met and will not be lost from sight in practice? - For projects a tailor-made ethics code of conduct that includes ethical values as well as legal issues must be developed before research activities are done:

The code of conduct serves a common understanding and therefore its rules need to be agreed on by all researchers who have to deal with it. This is especially important for cross-national research, when laws, declarations and standards differ. But not only because of ethical aspects it is so important, also in the sense of scientific work with valid results: only in the case the researchers and the participants in all participating countries have the same level of information and feel comfortable with the research action data will be valid and comparable. The Code of Conduct in cross-national research protects the professional integrity of the

researchers, their employers and the scientific community as well as the participants and the social community (see Freed-Taylor, 1994).

Further, Deborah Smith (2003) published the American Psychological Association's strategies for steering clear of ethical dilemmas that can be useful as first advisor also in social research:

1. Discuss intellectual property frankly
2. Be conscious of multiple roles
3. Follow informed-consent rules
4. Respect confidentiality and privacy
5. Tap into ethics resources

# 6 Models for Ethical Evaluations

Ethics and ethical issues are an area that is not easy to catch, work with and to keep in mind in development steps – even if rules and regulations are reflected and in our minds. One reason for this is an unsystematic and unstructured practice. To avoid ethical collisions in the project, PALAEMON's approach is the use of a model (EESSR), an adapted version from the field of Active and Assisted Living that was already used successfully.

## 6.1 MEESTAR

MEESTAR (Model for the Ethical Evaluation of Socio-Technical Arrangements) is an analysis framework for the ethical evaluation of the implementation of assistive technologies in life worlds. The instrument is based on the work of Manzeschke, Weber, Rother and Fangerau (2013), who developed MEESTAR in a study accompanying Active and Assisted Living (AAL) projects.

Its values are to make the topic of ethics more concrete and to present an easy and useful guideline how to catch ethical aspects that need to be taken into account ongoing from an very early stage of an technological development for the health care sector. MEESTAR describes preconditions which are crucial for the development and practicability of systems from an ethical point of view. Further, the instrument supports the identification of possible ethical undesired consequences and fosters the finding of solutions to avoid these outcomes.

Ethical areas of tension in this context and where MEESTAR can be deployed are diverse; for example: Has the technology intrinsic disciplinary measures? Does the socio-technical system cause burden or relieve for users? Does the system foster autonomy, does it give assistance and what happens if malfunctions occur? Does the technology overrule equal chances? Does the use of the technology encourage the change of individual and societal structures of welfare?

For answering these and further questions from an ethical point of view, topics related to the (planned) development are categorized and bought in line with the dimensions for the ethical assessment (x-axis) and following, in combination with the levels of impact (z-axis) and in regard of the users' perspectives analysed.

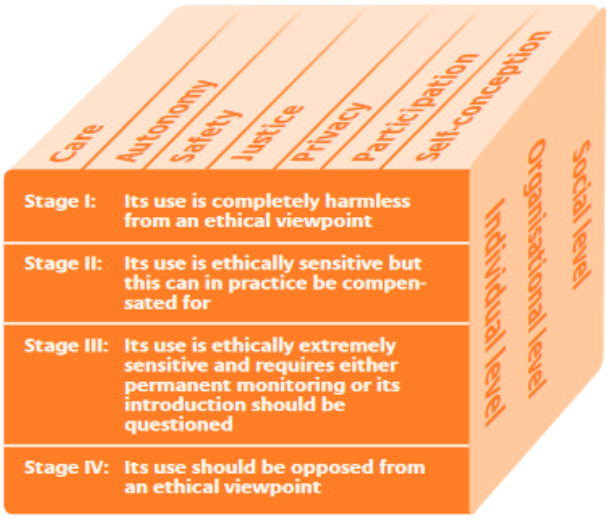


*Figure 1 MEESTAR Modell (Manzeschke et al., 2013)*

### 6.2 EESSR

The safety and security sector is an area, where a lot of innovations come along with the new technologies. Also here, the effective interaction between humans and technologies is crucial in the sense of life-saving and avoiding burden - for all persons involved. In this context it's not only important if things work, also ethical aspects must be taken into account at a very early stage of development (planning phase) and also ongoing during the development; also for meeting the needs of an solidary ideology that this sector implies. It is necessary to have assessment tools that are easy to use and – more important – that make a systematic analysis possible.

However, in the safety and security sector such an easy to use model for analysing ethical aspects in technological development-phases was missing but needed.

Therefore, the evaluation tool MEESTAR (see 6.1) was adopted for this area by Georg Aumayr (JOAFG, 2019), who is experienced in both fields, ethics for AAL as well as safety and security, and gave the amended instrument its name: Ethic Evaluation Standard for Security Research (EESSR).

Like MEESTAR, EESSR fosters the identification of ethical issues in advance or during the development and supports to take them into account in further phases as technology systems and/ or its elements must be sketched and subsequently discussed in regard of their influence on ethical matters. Further, it enables the users to structure, assess and allocate ethical issues to relevant tasks and facilitates a reflexion and the visualising of ethical aspects for relevant finished tasks. But most important and wide-ranging, the developers get sensitized for the topic and a common understanding about the vision and the importance of ethical considerations is created.

Following main questions define the application areas, support the understanding and make its necessity more transparent:

- Are technologies used or related research processes critical from an ethical point of view?

- Which specific ethical challenges arise from developing, testing and using the technology?
- Can the defined ethical issues/ problems be mitigated or even solved? If yes, which potential solutions are possible?
- Are there ethical issues so critical that development, testing and/ or using the system has to be stopped?
- Have unexpected critical problems occurred, which have not been assessable before? How do you deal with them?
- Which aspects and functionalities need to be considered explicitly from an ethical point of view when developing, testing and using the system?

### 6.2.1 Structure of EESSR

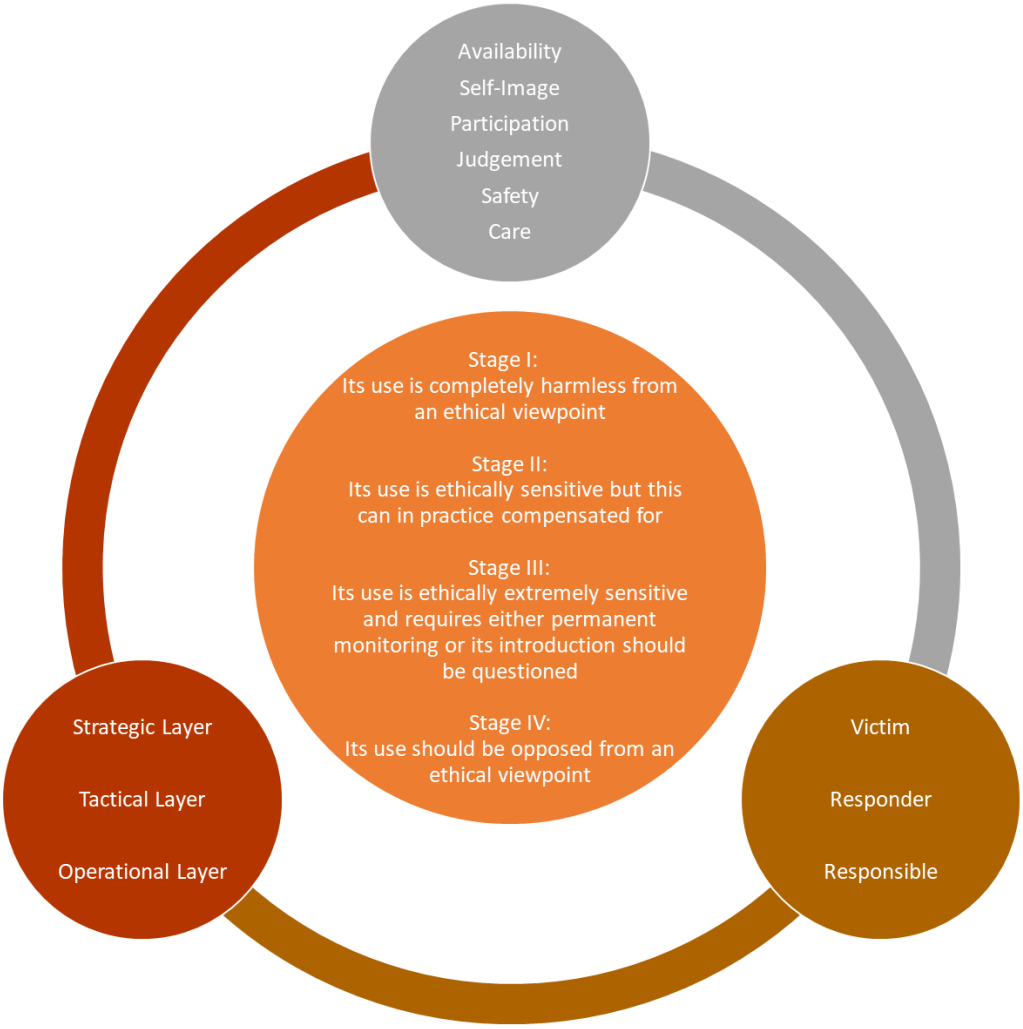


*Figure 2 EESSR*

As Figure 2 points out, it is all about the grades of the ethical relevance that are set in the centre and named by 4 stages:

| | |
|---|---|
| Stage I | Its use is completely harmless from an ethical viewpoint. |
| Stage II | Its use is ethically sensitive but this can in practice compensated for. |

| | |
|---|---|
| Stage III | Its use is ethically extremely sensitive and requires either permanent monitoring or its introduction should be questioned |
| Stage IV | Its use should be opposed from an ethical viewpoint. |

Each description of the stages gives a hint what to do with the allocated issue in the upcoming steps of the development. The aim is to reach Stage I for each element; only then the technology system is marketable from an ethical point of view.

On the top of the outer circle the dimensions of the ethical assessments are placed. The ethical questions and issues that come up in the discussion must be categorized according these. To create a common understanding on what these dimensions include; following some examples for each term:

| | |
|---|---|
| Availability | Readiness, capability, standby, attendance |
| Self-image of the User | Self-assessment, weaknesses and strengths, skills |
| Participation | Teamwork, cooperation |
| Ability for Judgement | Mental stability, knowledge, training |
| Personal Safety | Self-responsibility, control |
| Care and Support | Helpfulness, solidarity, altruism |

In the outer circle of the figure three users (victim, responder and responsible) are listed. When applying EESSR the perspectives of those three actors must be assessed. Further, the strategical, tactical and operational layer build the levels on impact. Also, all three must be seen and the ethical questions discussed for each level.

At a very first sight – especially when looking at Figure 1 and Figure 2 - MEESTAR and EESSR seem to be quite different. But, in fact both models are very similar: of course it was necessary to adopt the wording for the safety and security sector. Further, the figure of EESSR displays additionally the perspectives that need to be taken into account. However, the application could be taken over for EESSR and is the same as for MEESTAR. This was important, as it can be expected by this that EESSR works in a same manner with a systematic discussion on ethics accompanying the whole technological development as MEESTAR.

### 6.2.2 Application of EESSR

In a first step ethical questions and issues that could be relevant and are related to the technology must be identified and described. At best this should be done in an interdisciplinary group of experts who are needed and involved for/ in the development. By this it is guaranteed that all professional perspectives are covered.

Secondly, the ethical relevant issues that came up in the prior discussion have to be categorized to the dimension of the ethical assessment (availability, self-image, participation,

etc.). It may occur that one or more issues could fit into more than one category. In this case the main dimension represented must be identified and chosen.

In a next step, the ethical questions and issues need to be categorized according to the layers of EESSR:

- strategic: means a long-term planning for preventing bad situations
- tactical: means the controlling and planning of actions
- operational: means working at the place of action

Then their ethic gravity according to the four stages have to be evaluated.

The last step is then, to allocate the findings to the phases of the development and its tasks for keeping them in mind and for considering them in all processes of the development.

Like the usage of MEESTAR, EESSR should be applied in an early phase of the technical development at first and then periodically discussed in workshops across the development according to its state.

By doing this, it should be ensured that the ethical issues and questions are adjusted. However, EESSR-results must be treated like a living document and revised regularly!

# 7 Conclusions

It has been shown that ethics and legislation are closely linked in our social cultures and therefor also in social science. The presented work displays the base for ethically and legally correct acting within the project and its trials and makes the consortium aware of the existence of rules and regulations.

The document shows that all dimensions have been taken into account:

1. Operational dimension:
   The topic of the project and the environment in which it will be implemented,
2. Technological dimension:
   The technologies and the system concept of operation,
3. Project implementation dimension:
   The conduct of the project, including partners' and external persons' code of conduct and behaviour,
4. Data Management Plan:
   The management of the project data sets during and after the project.

The examination with this topic has shown that there are several issues to be taken into account during the technical development phase and in the trials as well as in the trial preparation phases not to harm any project partner's (in person) and/ or trial participant's rights and confidence.

EESSR is the chosen ethic evaluation tool that will accompany the project and the consortium for making visible and thus aware of ethical issues concerning the technical developments, the trials but also the product in future that is developed for saving lives, in all phases of PALAEMON.

Furthermore, by its content, this deliverable serves as theoretical background for D1.8 Ethics Manual and Guidelines for data protection and safety on passenger ships.

## 8 Sources

All European Academies. (2017). The European Code of Conduct for Research Integrity. (Revised Edition). Berlin, Germany. Retrieved February 2020, from https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf

Consortium of PALAEMON. (2018, September). *PALAEMON submitted proposal version.*

DESCA, adapted by the Consortium of PALAEMON. (2019). *DESCA 2020 Model Consortium Agreement* (PALAEMON Consortium Agreement, version 2.0 ed.).

EC Innovation and Networks Executive Agency. (2019). *Grant Agreement Number 814962 - PALAEMON.*

European Commission. (n.d.). *Responsible research innovation | Horizon 2020*. Retrieved February 2020, from https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

European Commission. (n.d.). *What is personal data?* (E. Commission, Editor) Retrieved January 2020, from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

GDPR.EU. (n.d.). General Data Protection Regulation (GDPR). Proton Technologies AG. Retrieved January 2020, from https://gdpr.eu/tag/gdpr/

International Civil Service Commission. (2013). Standards of Conduct for the International Civil Service. New York. Retrieved January 2020, from https://icsc.un.org/Resources/General/Publications/standardsE.pdf

International Maritime Organization. (2016). Code of Ethics for International Maritime Organization Personnel. Retrieved January 2020, from http://www.imo.org/en/OurWork/Documents/Code%20of%20Ethics%20for%20IMO%20Personnel.pdf

International Maritime Organization. (n.d.). *Introduction to IMO*. Retrieved January 2020, from http://www.imo.org/en/About/Pages/Default.aspx

Manzeschke, A., Weber, K., Rother, E., & Fangerau, H. (2013). *Ergebnisse der Studie "Ethische Fragen im Bereich Altersgerechter Assistenzsysteme".* Berlin: VDI/VDE Innovation + Technik GmbH.

RESPECT project. (2004). RESPECT Code of Practice for Socio-Economic Research. Brighton, GB. Retrieved January 2020, from http://www.respectproject.org/code/respect_code.pdf

The Council of the European Union. (2013). Charter of Fundamental rights of the European Union. (E. Commission, Ed.) Brussels, Belgium. Retrieved January 2020, from http://data.europa.eu/eli/reg/2013/216/oj

The European Parliament and the Council of the European Union. (2002). Directive2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). (E. Commission, Hrsg.) Brussels, Belgium. Abgerufen am January

2020 von https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

The European Parliament and the Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *General Data Protection Regulation*. (E. Commission, Hrsg.) Brussels, Belgium. Abgerufen am January 2020 von http://data.europa.eu/eli/reg/2016/679/oj

World Health Organisation. (2001). World Medical Association Declaration of Heslinki. *Bulletin of the World Health Organisation*(4), p. 79.

World Medical Association. (2018). WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects. Retrieved January 2020, from https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/