D3.13

Analysis of Societal Acceptance and Ethical Acceptability – Issue 3

Instrument	Collaborative Project
Call / Topic	H2020-SEC-2016-2017/H2020-SEC-2016-2017-1
Project Title	Multi-Hazard Cooperative Management Tool for Data Exchange, Response Planning and Scenario Building
Project Number	740689
Project Acronym	HEIMDALL
Project Start Date	01/05/2017
Project Duration	45 months
Contributing WP	WP3
Dissemination Level	PU
Contractual Delivery Date	M45
Actual Delivery Date	05/01/2021
Editor	Lena Schlegel (EKUT)
Contributors	Prof. Dr. Regina Ammicht Quinn, Friedrich Gabel, Solange Martinez Demarco (EKUT)

Document History			
Version	Date	Modifications	Source
0.1	30/10/2020	First draft	EKUT
0.2	11/11/2020	Second draft	EKUT
0.3	17/11/2020	Third draft	EKUT
0.4	21/12/2020	Fourth draft	EKUT
0.5	23/12/2020	QA-Ready Version	EKUT
1.0.F	05/01/2021	Final version for submission	DLR

Table of Contents

List of Acronyms

C&C	Command and Control Centre
EKUT	Eberhard-Karls-Universität Tübingen (University of Tübingen)
EU	European Union
IN-PREP	INtegrated next generation PREParedness programme for improving effective inter-organisational response capacity in complex environments of disasters and causes of crises (H2020 project: 740627)
MRPP	Mixed Reality Preparedness Platform
PPDR	Public Protection and Disaster Relief
PSCE	Public Safety Communication Europe
UN	United Nations
UK	United Kingdom of Great Britain and Northern Ireland
WP	Work Package
VOST	Virtual Operations Support Team

Intentionally blank

Executive Summary

This deliverable is the third and final issue reporting on ethical acceptability and societal acceptance of the HEIMDALL system. In this issue, the framework on societal acceptance and ethical acceptability developed in [6] and [7] is summarised and complemented with insights from further empirical findings and observations throughout the development process.

Firstly, a summary of the theoretical aspects of societal acceptance and ethical acceptability drawn on in the context of this series of deliverables is provided, as well as an overview of the methods used for gathering and evaluating empirical data.

Based on the overall empirical findings, the emphasis of this deliverable lays on aspects related to the diversity in disaster management organisations and the different structures of disaster management across EU. The main – in part, new, and, in part, amplified – topics identified as important for the societal acceptance and ethical acceptability of HEIMDALL include: 1) Legal Frameworks to support the implementation and mutual adaptation of the system and the organisations; 2) Trust in the system; 3) Modes of Communication; and 4) the design of the system for cross-border communication, as well as cross-cutting aspects such as commercialisation, data quality, privacy, and security.

Although these aspects are issues on their own, they are also intertwined and hence their analysis continuously references other points. In particular with regard to (societal) acceptance, there are also important links to human factor aspects presented in [5]. As the system, in contrast to prior understanding, will not imply interaction with citizens, it has been concluded that contextual conditions of the machine-user-interaction will generate the framework for its acceptance. Hence, while this new understanding of the tool has led to some changes in the methodological approach, which saw one focus group replaced by a workshop and complemented by results from the interviews undertaken in the context of [5], empirical saturation has been reached supporting a theoretical framework for an ethical and societal acceptance of the system.

Finally, some concrete recommendations have been made with regard to moving from a prototype stage to the final product and making certain the societal acceptance and ethical acceptability of HEIMDALL. Ensuring that feedback from the end-users is taken into account in any further development of the system is an ongoing challenge in that respect. With regard to the implementation of the system, both the way of commercialisation, and the diverging legal and organisational frameworks across the EU need to be considered to allow for both harmonisation and demand-oriented support of disaster management processes. The value of trust in a system and the modes of communication and interaction among end-users as well as with the platform should not be underestimated when determining the final design and commercialisation. Finally, data quality, data protection and security measures are vital points to prevent misuses, injustices and ensuring societal acceptance.

1 Introduction

HEIMDALL is a platform ultimately designed to support disaster management processes and thereby contribute to the greater good of societies. Therefore, apart from the technical requirements necessary to get the system running, [3] stressed that also issues in terms of ergonomics and broader human factors ought to be considered in order for the system to correspond with the needs and requirements of its end-users. According to the overall concept of HEIMDALL as a technological system interacting with societal actors, it was further specified that these requirements are connected with the contribution (positive/negative) and the influence that HEIMDALL can produce in a vision of a good life for everyone (see Figure 1-1).

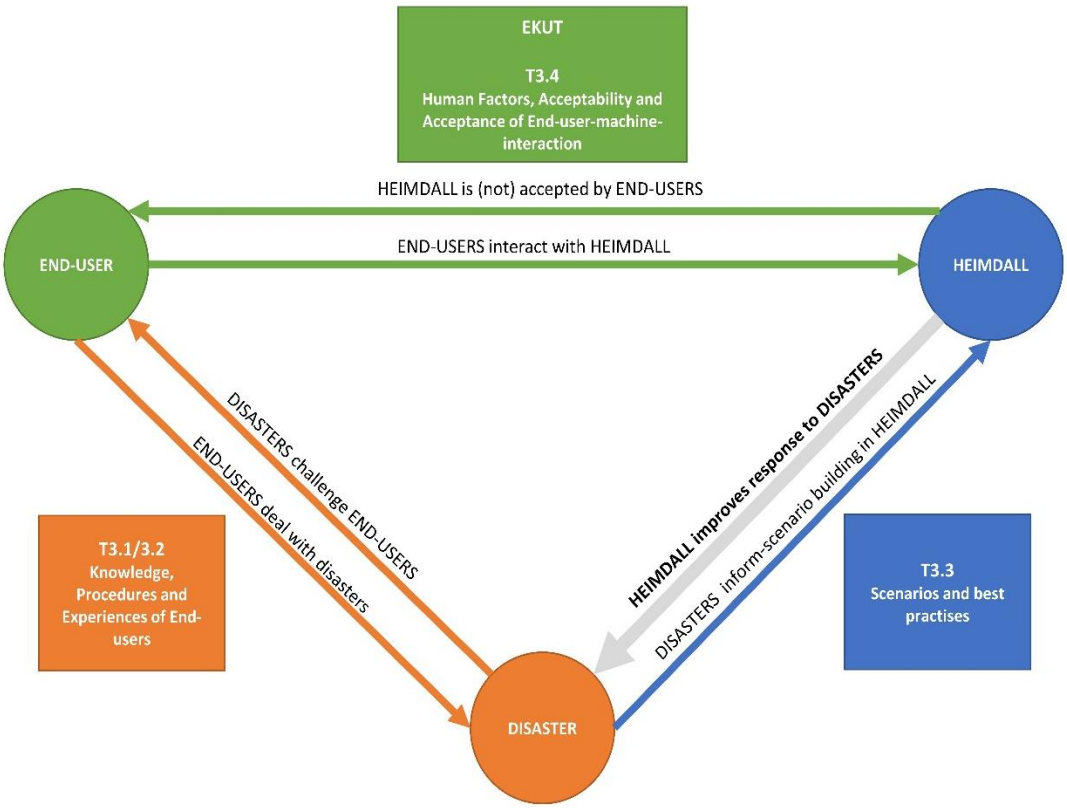

Figure 1-1 The role of WP3 in HEIMDALL (own compilation)

In order to achieve this aim, a theoretical framework for dealing with potential issues that might arise in terms of societal acceptance and ethical acceptability of HEIMDALL was devised in [6]. In [7], it was argued that given the potential effects of a technological intervention such as HEIMDALL on the common good of a society, discussions on the visions and aims involved in the development of the HEIMDALL system involving end-users, other stakeholders, and the broader society are required in order to adjust the development process along visions of a good life for everyone.

As the system will not imply direct interactions with citizens, the understanding of the tool and its acceptance has been slightly modified in comparison to previous deliverables. Hence, this final deliverable on societal acceptance and ethical acceptability focusses on the contextual conditions of end-users interacting with HEIMDALL as framework for its acceptance.

Consequently, the first part of this deliverable provides a summary of the theoretical framework adopted to analyse societal acceptance and ethical acceptability (chapter 2), and outlines the methodology used for gathering and evaluating the empirical data (chapter 3). In this vein, some changes in the methodology are elaborated, i.e. the replacement of one focus group with a workshop and the condensing of the empirical work into four items due to the empirical saturation in the proposed framework for ethical and social acceptance of the system. This resulted from the many overlapping and interlinking aspects which arose with relation to the

interviews undertaken as part of T3.4, and the rich observations from consortium discussions throughout the length of the project.

The main (new) empirical findings which are largely centred around aspects related to the diversity in disaster management organisations and the different structures of disaster management across the EU, are compiled in chapter 4 and include questions on: 1) Legal Frameworks to support the implementation and mutual adaptation of the system and the organisations; 2) Trust in the system; 3) Modes of Communication; 4) The design of the system for cross-border communication which are reinforced by cross-cutting aspects such as commercialisation, data quality, privacy, and security.

Finally, in chapter 5, the deliverable provides concluding remarks and some recommendations regarding requirements which should be taken into account for the final design, implementation and further development of the HEIMDALL system.

2 Societal acceptance and ethical acceptability

2.1 Societal acceptance

The results presented in [6] and [7] were built on a theoretical concept of societal acceptance as “a favourable or positive response (including attitude, intention, behaviour and – where appropriate – use) relating to a proposed or in situ technology or socio-technical system [in this case, HEIMDALL], by members of a given social unit (country or region, community or town, household, and organization)” ([23]: 9). While this definition has been adhered to throughout the research process, a shift has occurred in the unit of analysis. Whereas early assessments of both, the analysis of acceptance and the identification of Human Factors for HEIMDALL, included the possibility of interaction with citizens, it was later clarified that the system as such would not be accessed by members of the public or political decision makers. It can, however, contribute indirectly to political decision-making procedures by supporting the end-user organisations carrying out disaster management operations relevant to broader society. Likewise, while there will be no direct interaction of HEIMDALL with citizens, as it was also mentioned in [4], it can potentially play a role for enhancing communication with the public before, during and after crisis events.

Hence, (societal) acceptance of HEIMDALL goes beyond the mere human factors relevant for end-users´ interactions with it, but since citizens will not be directly interacting with it, it is the framework conditions of the respective environmental and societal context of its implementation that will generate its acceptance. Therefore, this deliverable focusses on these contextual conditions of societal acceptance for HEIMDALL, as observed in focus groups, interviews, a workshop and consortium discussions.

Because societal acceptance has been studied in a multiplicity of fields, there is a vast diversity of research methods that can be used for this purpose. In the case of HEIMDALL, focus groups were originally selected as means for analysing the societal acceptance of the system in order to focus on understanding the broad spectrum of stakeholders involved in the project and their attitudes, opinions, behaviour, intention, and use of the system [23]. The overall objective, thereby, was to elaborate on the values, attitudes, opinions, concerns, behaviour, and potential uses that HEIMDALL generates in those most likely to be affected by it. Based on the modified understanding of HEIMDALL’s interactions with society, these included mainly end-users, technical staff and other experts in the field of disaster management. Moreover, unlike initially planned, considering the changed understanding of the societal acceptance conditions of HEIMDALL, no focus groups were undertaken with citizens. Instead, further insights were gathered through a workshop, jointly organised with IN-PREP, another EU project, focussing on the ethics and policy of transboundary disaster management platforms.

This dynamic development of the research process also highlights one of the core aspects of societal acceptance as a concept, outlined in [6] and [7]. Societal acceptance is a process, which develops together with the development of the system. In this sense, it stresses the importance of the diversity of the social groups affected by it and their respective contexts, e. g. historical, institutional, social, economic, and geographical conditions (at local, national and European level) [23]. Considering that the project concludes with the development of a prototype, rather than a finalised technological system, it is argued that its societal acceptance will very much depend on its implementation at particular locations and in particular contexts.

Overall, it has become clearer throughout the project that societal acceptance is a complex concept that requires an understanding of the different factors that play a role when studying its empirical manifestation. The combination of focus groups, a workshop and insights from interviews and consortium discussions has offered a rich empirical base for developing the framework for HEIMDALL´s acceptance. Therefore, this deliverable aims to provide an overview of the diversity of factors and potential points to consider when implementing HEIMDALL across the diverse field of disaster management in the EU.

2.2 Ethical acceptability

In [6] it was outlined that besides considerations on social acceptance, of which moral beliefs and attitudes are one aspect, there is another way in which ethics are of importance for technology development. While acceptance refers to the question of "What is?" or "What is to be expected?" – How do (in the case of HEIMDALL) end-users accept the HEIMDALL system? and, if not, what are the factors that negatively affect their attitude towards the system? – acceptability is about asking "Is something acceptable with regard to the normative values and beliefs of European citizens?". In other words, does the design of the HEIMDALL system contribute to existing ideas of a world where Europeans want to live in? [24]. As this formulation already suggests, this is a question which cannot be answered lightly or by a single person. Instead, to give an answer, one firstly needs to understand how the HEIMDALL platform works, secondly identify affected value dimensions, and thirdly start a discussion about the ways in which challenges are raised by the technology in question and how they might be addressed.

Against this backdrop, the consultation on the ethical acceptability of the HEIMDALL platform was an ongoing process which involved discussions with all partners in order to gain an understanding of what is needed on the operational ground and in how far technology is able to contribute to achieving these goals. With regard to the affected values, in previous deliverables three dimensions were deemed important for the HEIMDALL project: justice, responsibility and privacy. In the course of development of the project though, the normatively relevant aspect of trust, which had previously been understood as part of the justice dimension, evolved into a fourth important dimension on its own. Along these overarching values, ethical requirements for the acceptability of a system such as HEIMDALL were identified and elaborated throughout the project.

Justice refers to the overall aspect of the importance of a non-discriminatory disaster management, both on a social (discrimination of certain individuals and social groups) and on a societal level (discrimination of certain communities, municipalities or countries). Although in sections 2.1 and 3.1 it is outlined that the public is not to be considered as a 'direct' stakeholder, it is an interested party in relation to the development and deployment of the HEIMDALL platform. Therefore, even if the platform does not directly interact with the individual members of society, the positive and negative effects of using it do have an impact on individual vulnerabilities in extreme events. The same holds true for a more systemic level. Although HEIMDALL will only be used by those involved in disaster management, its use might well affect society on a broader level, leading to cascading events.

Consequently, in [6] it was argued that by using the system, existing disadvantages or discriminations of persons or groups should not be increased, better still reduced. In this regard, it was for instance advised to consider accessibility issues of the system. With regard, for example, to the UN Sendai Framework for Disaster Risk Reduction, disaster management should aim to be more inclusive and to allow, for instance, persons with disabilities to become part of disaster management processes [22]. For the HEIMDALL platform this refers to considering different features of the GUI, for example, providing an option for persons with red-green visual impairments (dyschromatopsia). Similarly, to allow accessibility the user language is of major importance, as for instance the exclusive use of the English language puts users from non-native speaking countries at a disadvantage. Furthermore, justice related challenges can be referred to in terms of fair pricing. As all individual members of the European society – as well as those the European Commission declared to protect when signing the Charter of Human Rights – are subjects to disaster prevention measures, there is a strong argument for ensuring access to the HEIMDALL system to all member states and disaster management agencies in Europe. Access not only via an equal availability and usability (in terms of, for instance, the user language as already explained) but also in a monetary sense, which would allow less wealthy countries to have the same level of disaster protection as richer countries. Finally, this refers to a more conscious consideration of side effects of security and disaster management

action and the question of who is paying the cost for disaster management measures. The HEIMDALL platform as a shared security mechanism, in this sense, is to be understood as one aspect of the European idea itself.

Responsibility has mainly been considered with regard to the accountability for the actions users of the HEIMDALL system take, the ways in which the HEIMDALL platform considers the existing responsibilities and decision-making rationales of end-users, as well as how the platform might shape these through its use. Here, the primary ethical requirement is that the system should not create responsibilities which are not possible to fulfil. Due to the very concept, a responsibility can only be attributed to a person, if this person is able to fulfil it. If instead a person is unable, for instance, due to a lack of capacities and/or capabilities, it would be ethically wrong to bear this responsibility in the first place. This, for instance, refers to the aspect of training for the use of HEIMDALL. As pointed out in section 4.1 in more detail, within the European Union there are multiple disaster management technologies, which demand appropriate training in order to be used. HEIMDALL was advised to connect to these systems – GUI and usability-wise – to reduce the training required as much as to promote appropriate training and responsible use of the software. Secondly, a requirement was formulated regarding the decision support. Here it was argued that operational decisions should not be simply outsourced to the HEIMDALL system but that decision support in terms of the rationales behind certain options should be transparent and that a human decision would always be necessary. Although not considered as an ethical value in itself, this interaction of transparency and responsibility is of great importance for HEIMDALL. This is not only due to the fact that transparency allows for an understanding of a technology and criticism, but also that high transparency might positively influence the usability and "intuitiveness" of the system [18]. This leads back to what was stated earlier regarding responsibilities that cannot be attributed. If the HEIMDALL platform does not allow for an understanding of how it works, a responsibility for a critical use and appropriate training might not be feasible.

This general idea of responsibility in the HEIMDALL project was further specified in four ways. Firstly, with regard to transparency of responsibility structures with which the system interacts. Secondly, by taking a look at the increased responsibility of disaster managers and/or authorities to appropriately use the data that becomes available through the system in order to improve disaster management efforts. Thirdly, responsibility was referred to in its interplay with questions of justice. Here especially the issue of which data is included in the system and which data is not was of importance. For instance, it was discussed to include data on vulnerable groups in certain areas in order to allow taking responsibility to equally consider their needs in disaster situations. Lastly, responsibility is associated with trust in terms of communication between end-users. Good communication is based on trust, which contributes to responsibility to be borne. In this sense, HEIMDALL should support processes of trust building and maintenance as much as communication, which in turn would support the use of the platform.

On the other hand, **trust** is not an ethical value in itself. Rather, trust is precondition for acting on an individual as well as on a societal level. Starting from a very basic idea of trust, e. g. not to be harmed when stepping outside and that established laws will still apply tomorrow, trust is able to reduce complexity by creating stability of fundamental assumptions of the world we live in ([1], [9]). This concept of trust is of a threefold relevance for the HEIMDALL project. Firstly, it is a key component of the research and development process, which includes the willingness to share information and data within the consortium and being honest about any limitations [18]. Secondly, as a condition for using the HEIMDALL platform, there has to be trust that the platform will work appropriately. Thirdly, trust might influence cooperation between European disaster organisations and the interaction with the HEIMDALL platform itself. In order to fulfil this threefold relevance, trust has to be rightfully earned and consistently scrutinised. For instance, taking a closer look on the main point here of trusting in the HEIMDALL platform, this means that in order to be acceptable, the platform has to keep its promise to provide reliable support for disaster management purposes, while at the same time an ongoing

critical examination and questioning of routines has to prevent blind trust or ignorance. Especially with regard to the decision support and interpretation of data it is of utmost importance to scrutinise the used algorithms and support mechanisms in order to be able to act if something does not work in an appropriate way. Hence, in order to generate trust, the HEIMDALL platform should allow to understand its algorithms and technology as well as to support the exchange with other users, for instance, in terms of having a shared user language.

Finally, **privacy** has been considered in the HEIMDALL project with regard to the major topic of protecting the operational data inserted, processed and used in the system. The main ethical requirement identified here was that due to the importance of this data for improving disaster management operations, a compromise had to be found that allows for accessing necessary data and sharing it with other stakeholders while at the same time preventing them from being mis-used by internal or external actors. Therefore, in terms of achieving an appropriate result, the ethical considerations regarding ethical acceptability followed a threefold approach. Firstly, it scrutinised the dimension of data security in order to prevent mis-use of the data by external sources. Secondly, under the headline of privacy and stakeholders, critical questions were asked about the necessity of specific data and/or a reduction of data. This especially included the use of personal data, for instance, in the way of anonymised or pseudonymised personal data. Thirdly, both dimensions were considered by pursuing an idea of privacy by design and therefore the consideration of its principles within the development process.

These dimensions and the associated ethical requirements have contributed to the identification and analysis of a variety of factors that contribute to the societal acceptance and ethical acceptability of the platform, as well as the recommendations made to move from the prototype stage into its implementation.

3 Methodology

3.1 Introduction

Following the description of societal acceptance and ethical acceptability presented in chapter 2 and [6] and [7], the empirical research undertaken aimed to evaluate the attitudes, opinions, and values of end-users and other experts held about the HEIMDALL system at different development stages (descriptive knowledge on societal acceptance) and their visions of how HEIMDALL should look like (normative knowledge on ethical acceptability).

Out of the five focus groups proposed in [6], three have been conducted with members of the HEIMDALL consortium in February 2018 in Milan (Italy) and their results have been presented in depth in [7]. As also explicated in [6] and [7], these focus groups with HEIMDALL consortium members have been conducted with the overall aim to provide a space for discussing in detail different understandings of technical and ethical issues and different visions of HEIMDALL prevailing among the consortium members and to evaluate them in terms of acceptance and acceptability.

Based on the previously mentioned changed understanding of HEIMDALL´s interactions with society, which does not, as previously anticipated, involve any direct interaction with citizens or politicians, the decision was made not to conduct any focus groups with these groups and instead to collect more data on the expectations and views of end-users and other experts in the field of disaster management beyond the HEIMDALL consortium. Due to budget constraints, the possibility to conduct focus groups has been limited to events such as international conferences and similar gatherings related to disaster management, where different potential participants (end-users and other experts) naturally assemble and are prepared to volunteer to participate in such a research.

In this sense, the fourth focus group was replaced with a workshop jointly organised by members of EKUT (HEIMDALL) and Trilateral Research, member of the EU project IN-PREP[1], as a part of the Public Safety Communication Europe (PSCE) Conference, which took place in June 2019 in Lancaster (England). The focus of this workshop was on identifying contexts, visions and challenges of implementing technological tools for improving disaster management operations in Europe across borders. The insights from this workshop presented in this deliverable highlight the main contextual conditions for implementing a tool like HEIMDALL, including legal frameworks, trust, communication and the specifics of cross-border cooperation.

The fifth and last focus group, planned to take place in March 2020 in Girona (Spain), during the final demonstration of HEIMDALL, has unfortunately been cancelled due to the ongoing COVID-19 pandemic. Because of the often repetitive aspects raised by participants in the focus groups and workshop – sometimes, the same topics were re-iterated for 20 minutes and up to one hour – this called off focus group was addressed to representatives of EU projects similar to HEIMDALL to avoid a redundancy of results. This occasion would have provided the opportunity to exchange with these representatives and to learn about their identified ethical and social challenges in order to elaborate a more complex picture in terms of social acceptance and ethical acceptability. Nevertheless, the interviews conducted in the context of analysing Human Factors, given the large thematic overlaps of this work with respect to matters of acceptability and acceptance have contributed further data and compensated for this

[1] The IN-PREP system is a collaborative training platform comprising (1) a Mixed Reality Preparedness Platform (MRPP); (2) training modules for testing coordination between agencies and their plans; and (3) a cross-organisational crisis management handbook. The project aims to improve collaborative response planning (preparedness phase), focussing on the lack of training capabilities and insufficient links in transboundary crises management [13].

shortcoming. Therefore, it can be confidently stated that research on the topic has achieved the point of data saturation, where no new themes and ideas can be identified.

3.2 Preparing, conducting, recording and evaluating the focus group discussions and workshop

As elaborated in [7], the three focus groups were carried out with the support of the project coordinator in the second half of February 2018 in Milan (Italy) during one of the HEIMDALL's project meetings. The number of participants per group was between 8 to 10 people who were actively involved and discussed about HEIMDALL for more than 1 hour and 20 minutes. Because the focus groups were conducted in English, which is not the mother tongue of many of the participants, this issue was considered throughout the development of the discussions, and afterwards, during the analysis and redaction of this deliverable. The format, guided by a loose questioning route but otherwise open, provided a vivid and rich discussion on the participants´ visions for HEIMDALL. The moderators intervened only to introduce the questions, keep control of the debates, avoid digression from the main topics, and to stick to the time schedule.

The newly introduced workshop was held at the PSCE Conference in Lancaster in June 2019. The workshop was organised in collaboration with Trilateral Research, a member of the EU project IN-PREP, also aiming to enhance disaster preparedness and cross-border cooperation. The major aims of this workshop were to understand and identify solutions – organisational and policy-related – that make the technology and transboundary, or inter-organisational collaborations work; and issues – ethical and societal – that need to be considered for such tools and the collaboration to properly function. Participants, which comprised both end-users and technical experts from the field of disaster management, were invited to bring an idea of a transboundary Public Protection and Disaster Relief (PPDR) experience, challenge or concern to the workshop which would then be developed into a concrete scenario. The objective was to better understand what kind of policy and inter-organisational concerns and challenges need to be addressed for novel transboundary PPDR technologies to support collaborative working. This approach allowed to put the focus on the contextual aspects of acceptance and acceptability outlined in chapter 2.

There were 7 participants in the workshop and considering the variety of methods used to gather ideas and opinions, participants were further split in several smaller groups with different discussions running in parallel. There was no strict questioning route as prepared for the focus groups, rather an array of open-ended methods loosely guided by the overarching questions. After a brief introduction of each participant and their relation to the topic/field, participants spent one hour discussing in small groups which problems could arise when using a tool such as HEIMDALL in a cross-border collaboration, without providing solutions to the mentioned problems. Aspects covered by this ranged from concerns about the tool going down; partners withdrawing from collaboration; language, organisational and legal barriers; and the preparation aspects required to facilitate such cooperation. In the next step, participants created affinity maps based on the answers to the previous section. They used *post-its* to write down and cluster these aspects into themes they defined in order to specify what kinds of preparation, frameworks and roles and responsibilities are required to make cross-border or inter-organisations collaboration effective using a new interoperable technology.

After that this activity was concluded and followed by a short break, members of both projects provided a brief presentation of each tool (10 mins approximately). In the subsequent hour, the participants were asked to develop a story of an event (like a scenario) anticipating some of the problems and challenges that appear when using a technology such as HEIMDALL in practice and identifying what kind of broader solutions these tools, then need to work properly. The goal of this "Design Fiction" was to identify, if participants imagined the perfect tool for transboundary training and crisis management, what else they would need in terms of information recommendation, processes/procedures, legal and/or policy framework(s), definition of responsibilities, language and business models to do transboundary training and response planning. Also, the focus was on understanding any possible differences between

preparedness and response phases in terms of using software and to identify solutions – organisational aspects and policy recommendations – that make transboundary collaborations successful or issues – ethical and societal – that need to be considered for such tools to work. Afterwards, 30 minutes were allocated for the participants to present their stories to each other, followed by another 30 minutes of broader group discussion around questions like what kinds of guidance and policy frameworks would be required in order for the tool to be useful and which shapes this guidance should take.

With respect to both the focus groups and the workshop, before the beginning of each event, the moderators briefly introduced themselves and the reasons for the research, handed out two copies of the informed consent forms to each of the participants and explained the need for recording the conversations. The moderators described the main rules within the discussions and the estimated duration. They provided basic information regarding their role as well as the importance of the participants' points of view. They stressed the idea that there were *no right or wrong* answers and that all participants had the same right to express their opinions. Also, the anonymity of the participants and the confidentiality of the analysis was guaranteed. Finally, participants had the opportunity to put forward any doubts about their participation in the event and the Informed Consent Forms. Afterwards, they signed the forms to verify their voluntary decision to be part of the discussions or workshop and their understanding of the reasons and rules stated in the forms. Once this last step was concluded the events started.

Subsequently, the recorded conversations were stored in an encrypted container and transcribed by members of EKUT. Due to the decision to anonymise, the transcripts are free of any personal or identifying information including potential names unintentionally mentioned during the discussions. The transcripts were evaluated following the descriptive-reductive content analysis method (see [14]: pages 183 et seq.) with the objective of summarising the main topics and arguments of the debates, reducing the data volume but increasing the amount of information. To avoid a potential subjective influence of the researchers on the results, all members of the EKUT team prepared their own analysis on each event which were then compared to produce a single consolidated evaluation. The selected themes and the corresponding relevant quotes to illustrate them will be presented in the following section.

4 Main findings

The ethical challenges identified at the beginning of the project [6] have been addressed continuously throughout the development process. However, it has also become apparent that new ethical issues and socio-cultural and legal concerns continue to emerge and may continue to emerge when the system moves from the prototype stage to its implementation in specific real-life situations and organisations. These socio-cultural and legal concerns are, of course, beyond technical solutions and require continuous adaptation from both partners: HEIMDALL and the organisation or institutional context in which it is adopted. In this sense, HEIMDALL can be either a facilitator or an obstacle to improving the overall crisis management system of the corresponding area. Due to the extremely diverse organisation of disaster management frameworks and organisations in the EU, these contextual conditions seem to be the key challenges for further developing and implementing HEIMDALL beyond the prototype stage. This final issue on societal acceptance and ethical acceptability, therefore, focusses on key areas where these differences play out and generate both conflict and potential for disaster management processes in the EU by a system such as HEIMDALL.

4.1 Legal Frameworks

The first area where these differences and potential issues with cross-border and inter-organisational collaborations have shown to play out significantly is the area of legal frameworks, which differ across the different member states of the EU and sometimes even between specific areas and administrative levels of one country. In this respect HEIMDALL provides potential for standardisation of disaster management operations across these different contexts, on the one hand, and may, on the other, encounter challenges with respect to accommodating the specific needs and requirements of each region and organisation.

Two main points have been identified in this regard, which should be considered in order to generate acceptance for the tool, if implemented. For one, mutual adaptation of the tool, organisational procedures and the corresponding legal frameworks is required to enable a successful implementation of the tool. And secondly, as data-sharing is one of the key benefits offered by HEIMDALL, respective frameworks regulating how data is being shared, with whom and what legal status it has in which contexts are required.

4.1.1 **Mutual Adaptation**

As end-users stressed in some of the interviews, in order to experience societal acceptance, HEIMDALL needs to adapt to the local legal, political and administrative contexts of the organisations using it.

First of all, it needs to consider the actual needs of the respective organisations it seeks to address. This was reflected in a discussion at the workshop where experts stressed that it might be more meaningful to combine HEIMDALL with existing systems/technologies of each organisation than to expect it to replace everything. It should account for the possibility that only a handful of the options that HEIMDALL offers are in fact necessary and useful for an organisation. While the modular structure of HEIMDALL is fit to accommodate such differences, this aspect should also be reflected in the business model, supporting the purchase of single modules which are compatible with other, existing technologies.

Furthermore, concerns were raised with regard to the current lack of interoperability because every organisation has its own system which may not necessarily correspond with one another. An example arose in one of the interviews, where a member of a Catalan hospital located at the French-Spanish border, making an analogy with HEIMDALL's implementation, stressed the difficulties of working under the peculiar European legal status which hosts two different legal and health systems under the same umbrella. According to the interviewee, it took 14 years from the time of first conversations until the idea of treating patients from both countries, including tourists, in the same hospital started to work. However, difficulties abound:

Ambulances cannot work at the other side of the border; medical degrees are not valid on the other side of the border due to insurance policies; medical records can be shared online via one health system that has very strict ethical and technical requirements to protect and access data, but not with the other. Also, the whole collaboration only works using three languages. The interviewee emphasised that agreements for collaboration are key to enable treating patients from the other side and that a system such as HEIMDALL should support and be supported by such agreements rather than pushing a completely new organisation. On this note, it was also emphasised in the workshop that in spite of a lack of interoperability due to the current differences in the technologies used by different organisations, cooperation can still be enabled if emergency plans are practiced and coordinated nationally.

These comments highlight the importance of mutual adaption between a newly introduced tool, the organisational procedures of the actors using it and legal frameworks which provide the basis for its use, in order to generate benefits and acceptance for HEIMDALL. Furthermore, in terms of acceptability it is recommended – in order to ensure a just and equal disaster management system to all members of the European Union – that this usability or connectivity of the HEIMDALL system to existing national systems is either ensured and monitored for all members of the EU, or that there are compensational measures in place that will help those disaster management systems which are not able to connect with the HEIMDALL system, to do so as soon as possible.

4.1.2 **Data and Data Sharing**

With respect to data and data sharing, end-users and other experts broadly agreed that it would be valuable to have access to lessons learnt or comparing scenarios from other areas in order to enhance decision-making processes and to use them for training. However, there were also concerns about the ownership of the data, its legal status and the question of accountability for its (mis-)use and for decisions made based on it.

In the workshop (and also in some interviews), participants stressed that a log of the decision-making process could be useful also in legal terms, as there are reviews, debriefs and public enquiries after an incident. End-users can then draw on a repository where to find lessons learnt or what to improve next time, and to support their accountability in case of legal proceedings, which can be useful to avoid a loss of confidence. However, the legal status of the system in legal proceedings is yet to be determined. For example, in one of the interviews a participant stated their concern that automated decisions suggested by the system would take away autonomy from incident commanders who have to be legally accountable for the decisions made. In contrast to an incident log, which is a legal document that can be used in court, the legal status of the system is not so clear: “Whereas, if you've got something, a machine, telling you this is what you need to do, you would need something to back that up, I would say. Because you can't go into court and say: Well the machine told me to do it.” (Firefighter, Station Manager, Scotland). Consequently, questions arise with respect to the role of the system in legal proceedings: Which kind of evidence can it provide – is it legally valid? And does it support or challenge the decision made? These kinds of questions need to be addressed by the legal bodies of the respective country using the tool in order to provide the context for its acceptance.

Another concern mentioned throughout the interviews, focus groups and the workshop was the danger of the tool serving as a function creep, for example, if the shared data is being misused for other purposes as to enhance disaster management operations. In this sense, the risk that insurances companies can get access to information collected, used, produced and stored in HEIMDALL is telling [7]. This question is also related to the commercialisation of the system, to which many participants expressed concern with regard to private businesses having access to data and profiting of it. Considering that many critical infrastructures are privately owned, there is doubt as to what degree this can be avoided. Consequently, it was also controversial whether there should be business incentives for using a system such as HEIMDALL.

Overall, the most pressing question which concerned all of the end-users was who would own the data and, consequently, who could be held accountable for potential misuse.

In sum, these results show that respective legal and regulatory frameworks are key to enable data-sharing between agencies and countries across the EU in a societally acceptable way. In addition, from an ethical acceptability perspective, it is recommended that legal norms for data-sharing are developed following the highest data protection standards of the European Union in order to ensure that these high standards are applied in the specific setting.

4.2 Trust

As participants stressed in the workshop, a successful incident management is based on trust – in people and technology – and procedures. One and the other go together and trust can also be in processes. Hence, the relationships among people and their interactions with the system and procedures are key for generating acceptance for the system.

4.2.1 **People**

As already stressed in [7] and further emphasised by comments during the workshop and interviews, it has been found that end-users draw their confidence from trust in interpersonal relations, organisational roles and structures, rather than trusting a technology per se.

A decision based purely on the suggestions provided by HEIMDALL was perceived by the participants as dissociated from the field and, therefore, not reliable. Trust in decisions, according to end-users´ statements in the focus groups, was derived from personal relationships and close personal communication because: “this relationship is between persons, not machines or platforms” (Participant, Focus Group). Besides training, this was also considered key for successful inter-agency collaboration by members of the workshop:

> *“This always helps in these areas. Because they have to trust each other. Especially if you think about mountain rescue. If you have somebody at the rope and the other one hanging down, he has to trust the other person. He has to know that they do the same, how they work together. Otherwise it doesn't work.” (Participant, Workshop).*

Moreover, the informal aspects of communication were valued higher in this respect than what can be enabled by formal communication:

> *“But the key thing that keeps the partnership going is good quality communication. And a degree of personal trust and personal relationships. I don't think we would have had stronger relationships if we had kept the communication at people level- was kept quite formal. The informal is more valuable at times than the formal bit” (High Scientific Officer, North Ireland Environment Agency, North Ireland).*

Supporting these statements, results from the focus groups hinted that HEIMDALL as a tool has its greatest value at the strategic level by providing and filtering information and facilitating the exchange and communication. Decisions, however, are taken at the tactical level by Command and Control (C&C) personnel. Therefore, HEIMDALL might reduce mistakes, but it cannot prevent them from happening and it cannot take responsibility away from human decision makers:

> *“So, I can run the scenarios back in the incident support room and give advice to a more junior manager or officer, but it's up to him or her to decide whether they take that advice or not. Now if they do something that goes wrong, I can step in and take charge formally. But I have to let them have their role, which is to make decisions on the incident ground. Because they will be actually there. They'll be seeing something that I may not be seeing and that's why I can't assume that my understanding is the same as theirs, because they're physically there.” (Firefighter, Station Officer, Scotland).*

In the opinion of the end-users, civil protection personnel rely on their experience and expertise rather than on technology, highlighting “the way we train our incident commanders, it would take that away from them. We need individuals making decisions” (ibid.).

It was further stressed that, if the system is perceived less reliable and efficient as current procedures, it would be disregarded. Furthermore, the end-users would have to know and understand the limits of the system in order to avoid confusion and panic in consequence of any misleading information the system might provide. For example, one end-user stated in an interview that using the tool to decide should take less time than through the current procedures without HEIMDALL: “It's true, we need something that can be used very quickly, that can give us what we need, saving our time, which is probably- this is another must of any platform. You should not invest more time than using no platform” (Firefighter, Director Coordinator, Italy). Then, if the time and effort required to take a decision based on the system is larger than without, the system is not considered an asset. What is more, participants of the workshop stressed that society would trust in the system as it displays the human decision makers, rather than in the tool itself, “because, it doesn´t come from HEIMDALL, it comes from the decision makers, from the authorities” (Participant, Workshop).

In this sense, as stated in [7] and aiming at a socially acceptable system, the emphasis should be on supporting current responsibility structures and working for better communication and cooperation via generating trust in the system and the people working with it.

Furthermore, in terms of ethical acceptability this means that this trust should be understood as of a reflective kind. On the one hand, there should be a consistent critical examination of the system in order to prevent blind trust or, in other words, to ensure that existing responsibility structures do still exist and are not outsourced to the system. On the other hand, this type of trust also implies the adoption of an open culture of discussing errors and mistakes due to either the platform or the end-users. In this second case, it implies that the logs where those mistakes and errors are recorded, can be shared. Both aspects would support a constant improvement of the system and, on a more general level, the disaster management procedures as such.

4.2.2 **Quality of Data**

The second key aspect with regard to trust is, once more, that information is always incomplete, might be inaccurate and, consequently, the system can only be as good as the information it collects:

> *“The important thing is […] making sure that the information that is fed into the platform or the module is- how good is it? You know, we would have a saying here in Northern Ireland of ´if you put rubbish in, you get rubbish out´. So, if its […] good quality data that is going in to allow the modelling, then you'll get good modelling” (High Scientific Officer, North Ireland Environment Agency).*

Relating back to the results already presented in [7], trust in the data provided by the system is based on its generation following known and tested processes and from known sources, including other end-user organisations and own information, fed into the system. In this sense, end-users raised their concerns about generating a common picture of a situation among different agencies using different kinds of data as a decision-making basis:

> *“One of the biggest issues, I think, is working with the same map material, mapping material. Because the Fire Department is organised as it is, as an independent company, it's owned by the municipalities, but we are not a part of the municipalities. That means that we don't necessarily have access to their geographical information systems or that platform. We have to ask for each and every time or we have to have an employee from each municipality, an expert, sitting at his or her laptop. But we can still have an incomplete map if it covers more than one municipality […]. So, that gives us the challenge of providing the same level of information to all participants. We don't have the same situational picture, so to speak. We can put it together from lots of pieces but that takes a lot of time and then the situation changes and then you just start all over again. So that is a major problem or issue that we have to deal with” (Firefighter, Denmark)*.

The sharing of common data across agencies can thus enhance the quality of the overall information base for making decisions. However, as stressed in section 4.1.2, legal and

regulatory frameworks should be in place to enable and structure this information sharing, which again can enhance trust in the process and in the quality of the data provided.

As mentioned in previous deliverables on acceptability and acceptance, but also in the context of human factors, HEIMDALL is expected to present information in a structured and reduced way to limit the mental load for decision makers. This is a key requirement in order for the platform to be considered useful; too much information can be overwhelming and lead to more confusion rather than a more structured decision-making process. However, it was stressed with equal emphasis that information should be presented without indicating preferences, so that decision can be based on information as little biased as possible:

> *"My concern, and I've mentioned it in a few meetings now, is that there shouldn't be put in any form of hierarchy, the outputs of HEIMDALL shouldn't be in a hierarchy, because then it points towards one of the tops, the best one, and if they're numbered, number one is the best one and if you choose number three then why did you not choose number one? So, I have a concern about how the information is displayed to the user, because the decision always has to come to, not even me, to the incident commander" (Firefighter, Scotland).*

This transparency of the data presented is vital for the end-users to trust in the system. Possible ways to ensure this transparency that were also already stressed in [5] and continuously re-iterated in consortium meetings include clearly indicating the parameters and weights used to produce simulation results and to allow users to manually refine parameters and weights.

Also, relating to what has been stressed in section 4.2.1 about the need for human accountability for decisions made based on information provided by the platform, transparency of how certain decisions came to be made is also important after the incident: "This has to be transparent and finally, your system cannot make the decision. This has to be done by a person- by the responsible person" (Research and Technology Projects Manager, Luxembourg).

Once again, a log documenting the steps undertaken in the system was considered an important asset to ensuring such transparency:

> *"So, when we make a decision, we put what the decision was, why we made that decision and any rationale. So, I would simply enter that I made a decision based upon the information from HEIMDALL and the rationale was that, after running scenarios, my choice was to select scenario X. Because, in my opinion, it gives the best result. That would just be entered into my log. […] I think what it [HEIMDALL] should do is provide- If I've chosen scenario X, […] somebody is going to say, well show me scenario X. And show me the other ones you looked at the same time, so it should definitely have them stored so that I can reference to them and somebody else can look through and see whether my decision was justified or not" (Firefighter, Scotland).*

Another aspect affecting the ethical acceptability of the tool related to the quality of the data refers to security of the data. Participants in the workshop raised a severe concern of data leaking or breaches. A data leak, in this context, would not only imply violations of personal data security but could also cause misinformation or panic in case information gets to the public and is misinterpreted, leading to inaccurate perception of an incident or to reputational issues for the organisation. This assessment corresponds with insights from the literature review, which found that a lack of engagement with the public can lead to disinformation and criticism [16]. Also, the participants of the workshop raised the risk of a deliberate data breach, such as from 'disgruntled ex-employees' who provide access to the platform to third parties after leaving the organisation. In this sense, security needs to be very well-considered, as misuse can be the consequence of someone gaining access to data which should not be available to them. Therefore, as stressed previously and participants confirmed in the workshop, access to data should be restricted, e.g. by vetting people to assign different levels of access to data:

> *"from a police point of view, we have different levels of vetting, and we have different access to restricted, confidential, sensitive information. So, for example, I´m vetted to a level, another colleague may be to a higher or a lower level, but you get some of the environment agencies not vetted, at all" (Participant, Workshop).*

This implies not just attributing roles with different access levels, but also to perform a clearance process to confirm that the person is trustworthy and aware of the protocols. Otherwise, sharing data can become a vulnerability.

Therefore, participants in the workshop stressed the point that policies, procedures and plans have to be up-to-date, including the resources, tying together training and information. Tailoring the system to the needs of end-users throughout different disaster phases can enhance confidence in its use. For example, an end-user stated in an interview that in the response phase, the system could be an improvement if it provides macroeconomic data that it is currently not considered; in the recovery phase, decision support could help standardising the process, e.g. which buildings to stabilise to restart working. Many other stressed that they would also like to use the system for training, which is considered an important aspect with regard to trust, as exercising with the system will generate confidence in it.

4.3 Communication

Related to the aspects discussed in both sections 4.1 and 4.2, communication has been identified as a key element to ensure the acceptance and acceptability of the platform. Emergency management is a highly volatile environment which stands under different pressures, such as time, uncertainty, unexpected developments of a situation, unfolding impact, and political and societal scrutiny ([8]; [11]; [15]; [17]). Emergency managers thus "rely on intense communication and coordination and structured processes that are heavily regulated" ([8]: 2). This involves the two-way communication between the platform and the user; the culture of communication prevalent in an organisation; the modes of communication between organisations or actors from different countries; as well as the communication with the broader public.

With respect to the communication between the platform and the users, participants stressed repeatedly that the data and information provided must be comprehensible across different levels in the hierarchy, between different agencies and regions involving different organisational cultures, linguistic differences, and regulatory frameworks, demanding a large translatability of the system. This aspect is strongly related to Human Factors as considered in [5], but goes beyond it because many of these conditions are contextual and depend on the system´s implementation rather than being aspects that can be considered at a prototype stage.

With regard to communication between agencies and with the broader public, end-users highlighted the necessity to consider the diversity of situations and established communication channels. For example, in Italy companies are by law required to provide information about what to do in specific incidents, but there is no comprehensive policy framework for this, rather it depends on the municipality and the types of industries in the area. Then, in an area where many high-risk chemical industries are situated, the communication required in case of an incident may differ from another area where these kinds of vulnerabilities do not exist. The information that needs to be shared also depends very much on the specifics of a given situation, which may not be reflected in pre-defined response plans deposited in the platform:

> *"If we have a hazardous materials incident where you have some cloud moving or some dangerous material moving, you need to be careful in explaining very well the situation. Being much more precise and giving much more understandable information" (Firefighter, Director Coordinator, Italy).*

Hence, the interviewee stressed that it would not be sufficient for the platform to send a warning stating that there is a chemical incident, but that a lot more is involved in communicating with the public in emergency situations that cannot be simply replaced by HEIMDALL: specific local public announcement systems including loudspeakers, traffic light signs, information signs, sirens and public communication systems. What is more, citizens in risk-prone areas should be kept informed about the risks and pre-defined response plans so they know how to act in an emergency.

> *"So, any citizen can access the risk map of his own area because the citizen needs and has a right to be informed of any risk. So, they are not secret, the maps. The maps that say, yes Sir,*

you live in a landslide prone area. Twenty years ago, it was a problem to say this (laughs). Now it's not any more a problem. People know that they live in a disaster-prone area. And they have to follow the plan that has been provided for their own specific area" (Ibid.).

Then, connecting these kinds of maps to the system would be a core benefit in terms of communicating with the public and preparing them for an incident in their specific area. The main concern here would be to ensure that the response plans provided by the system are up-to-date:

"That if you have a landslide in that area which has actually happened before, […] you already have a point for blocking the roads or diverting the traffic or how to serve and how to rescue isolated people. And it is written in the plan. But if the plan has changed, and in your platform, you are looking at the old plan, maybe there is some gap. […] [Therefore] there might be this problem of the data which is not updated" (Ibid).

Moreover, a tool like HEIMDALL can be utilised not only in terms of classical information sharing, but increasingly, attention of disaster managers also turns to the question of how to utilise the vast amounts of data allocated on social media in crisis situations. In this sense, HEIMDALL provides the possibility to connect with social media. The questions whether and how such data could and should be used was discussed among the consortium throughout the project. However, this is only a very recent development and many organisations are unsure about how to deal with it. In the interviews and consortium discussions, while acknowledging the added value of utilising near-real-time information coming from social media, end-users also mentioned serious concerns including lack of trust, data protection issues, and the current lack of organisational integration. An interviewee explained about the difficulty of determining the merit of social media data, while at the same time acknowledging the benefit of getting a feeling for how the public reacts to an incident:

"We supervise the social media, Facebook and Twitter and so on. But we don't blindly act on what is going on the social media. Because lots of, sorry for the expression, fake news […] but it [what social media says] goes through a lot of filters, what is happening out there. But it gives us a feeling of what's about in the public" (Firefighter, Denmark).

However, the interviewee further emphasised that as a firefighting agency they do not have the resources to analyse social media data on a larger and more systematic scale:

"Because we have plenty to do with just making ends meet on a daily basis. So, that would demand someone to do it because we don't actually have the resources to do it" (ibid.).

In this context, the suggestion to employ digital volunteers, such as Virtual Operations Support Teams (VOST) to work as trusted agents between civil society and formal emergency management [12] to collect and filter social media data for the organisations was generally considered useful. However, some end-users from the consortium dismissed this option due to the fact that they did not trust the VOST groups in their respective area. Controversies remained about the use of social media data and, consequently, the final decision has been made not to integrate social media data to the HEIMDALL system for the final demonstration, but to keep the possibility open for the development beyond the prototype stage. Considering that the importance of social media among the public is continuously rising, however, disaster managers are required to engage with the potential role of social media for crisis management both as a challenge and a potential "game changer" ([20]: page 59) and a useful resource for decision-making processes in crises ([10]). Therefore, this question should receive further consideration if HEIMDALL moves beyond the prototype stage. Considering the importance with which citizens rate the recognition of their contents generated on social media ([19]: page 106) and the emotional support that can be provided to citizens during a crisis through social media ([2]: page 5, [21]: page 612), engagement with this topic will be a crucial contextual element to consider for societal acceptance. After all, the controversies around social media highlight once more, how important trust related to communication is for the acceptance of a system such as HEIMDALL.

Lastly, it was emphasised repeatedly that the system could be used for training, both of personnel and with regard to preparing the broader public for specific incidents: “We'll start with joint principles. So, you need to have an agreement about how you will approach communication before, during and after, which will also inform the training and the involvement of people in the training” (Participant, Workshop).

With regard to informing the public about certain incidents, several agencies stressed that there is a need to educate population in specific risks and potential measures depending on their area. For example, a member of a Spanish environmental agency stressed that while citizens receive general information about incidents in the response phase, they lack specific information and training about how to act in certain situation or according to regionally specific risks:

> *“There are many types of plans. What I also see it’s that the information given to the population, in general, is too broad. There I see work to do. General information about what a risk is, [about] the problem that might happen is provided. But the specific information about how to act in that [particular] case or area, I think, in that sense, there’s much work to do” (Analyst, Environment and Water Agency of Andalusia, Spain, own translation).*

In the same context, a representative from an environment agency from the UK suggested that accompanying the implementation of HEIMDALL, the tool could be used to provide specific trainings for serious incidents with participation from civil society organisations and the broader public, for example with regard to developing skills in prescribed burning techniques: “We encourage land owners, farmers, to develop their own experience and, where possible, to get appropriate training on how to use fire as a management tool” (High Scientific Officer, North Ireland Environment Agency). Such utilisations of the tool could raise awareness for its value and increase its overall acceptance.

4.4 Cross-border cooperation

As a tool for the management of complex crisis situations, HEIMDALL aims to support procedures for inter-organisational coordination, including cross-border cooperation.

Throughout the interviews, the workshop, and consortium conversations, it became clear that, first of all, general agreements on collaboration need to be in place between the two respective countries in order to provide an enabling framework for cross-border collaboration altogether. These are essential to establish which actor pays and carries responsibility for what when supporting other agencies across the border and how insurance is provided for personnel involved. Among the participants, many stated that such agreements were already in place, for example, between Spain and Portugal; Spain and France; France and Germany; Ireland and Northern Ireland; the mountain regions between Italy and Slovenia, or Germany and Austria; as well as among the Nordic countries. These agreements provide the legal framework for collaboration and reduce bureaucratic efforts required to receive support from the other side of the border, e.g. in case of a request for helicopter, information, or personnel. For instance, a Danish fire department reported that based on the general framework for crisis assistance among the Nordic countries, a special agreement specifying how firefighters can work together was established, reducing bureaucracy and speeding up the request for help that would otherwise fall under UN or similar agreements.

However, while formal agreements generate the base for collaboration, they also create limitations for it. For example, a member of a Spanish environmental agency stated that, while collaboration agreements between Spain and Portugal were in place, in case an incident required help from the other side of the border, a political decision was required, as well:

> *Interviewee: “[…] Or there are also collaboration agreements with Portugal […] to provide support in case of fires that could be between one and the other site [Spain and Portugal]; that could affect both places.”*
>
> *Interviewer: “And in that case, is also political the moment when the request is activated?”*

Interviewee: "Yes, the decision can come recommended from the ground [the incident commander or similar position] […], but in the end, the decision is political. It is a procedure that implies the signature by those responsible and the submission of information. Once this has been processed, then the operative phase can be organised internally" (Analyst, Environment and Water Agency of Andalusia, Spain, own translation).

Also, sometimes such agreements only reflect a minimum consensus without each of the organisations giving up any individual responsibility and authority. For example, an expert shared their experience with the Italian-Slovenian collaboration agreement, which allows but for little sharing of information, such as a description of the incident, location of personnel in the field, and alerts, while both sides keep a copy and are responsible for the data shared. Limitations to sharing data are thereby dependent upon the respective country´s and agency´s rules, but also on differing mental models:

"It is privacy, but it is also the rules of each agency and each country on what information they want to share. And, in fact, I think, you know it, some agencies want to work or are open to share information, others are very closed. And if you, for instance, provide- the police is more reluctant than the fire brigade, for instance, with information. If you see location information from the police, nobody else will receive it. They never give out information about where the policemen are to anybody besides than internals. While fire brigades are first responders in a disaster, they are happy to provide this information because it can save their life if others know where they are. So, these are different concepts and if we have different agencies working together, everybody has to say: 'I can share this information, this information, or I share no information'. These are the responsibilities of the agency and how they work and what they are allowed to do, and it depends on the country. If the country is open, or if it is more reluctant to share" (Research and Technology Projects Manager, Luxembourg).

Therefore, participants stressed the necessity for more specific or agile agreements based on the local level. Successful collaboration experiences were reported especially in cases where close personal contacts and informal communication exist between the partners. In fact, personal contacts were seen as the solution to the limitations created by agreements. For example, a Catalan firefighting agency at the French-Spanish border reported that they maintained close informal contacts with firefighters at the other side of the border, including copying their structures and procedures for attending at an incident. According to them, these informal efforts paved the way for collaborating – also with the police – on cases such as mountain rescues, chemical incidents, etc. The fact that national agreements providing the framework for this collaboration have been in place since the 1980s, and later shifted more authority to Catalunya and to the local level, confirms the previous point. The final authority to decide over the sharing resources, however, remains with the national government.

In contrast, actors from Northern Ireland reported that a memorandum of understanding with Ireland about sharing information and helicopters was successfully implemented entirely due to personal contacts and informal conversations:

"[…] through a local- an existing memorandum of understanding between the two organisations, they already [have] their data, whatever data is shared accordingly. While I don't work with the Irish Fire and Rescue Services as such, I have a contact in the Irish government, […], and he is their lead wildfire person. Him and I would be on constant contact during the fire season, could be weekly, sometimes even daily, depending on how big the risk is. […] We haven't had any need to share any kind of personal data, but we would share information about locations of fires and that has actually been quite an important personal relationship for the department because […] the benefit of that relationship was, last year, for the first time ever, the Northern Ireland rescue service had to call in helicopters to help put out fires. The helicopters came from the Irish government, the Irish Air Corps. So, these were military helicopters from the Irish Army or Air Corps that were now flying in Northern Ireland to help [put out] wildfires. And that actually came about by me working at the ground level with this contact in the Irish Fire Service because it was through him that we could get the requests put through for- at government level to get that assistance brought up when it was needed" (High Scientific Officer, North Ireland Environment Agency, North Ireland).

According to the interviewee, the success of this collaboration was due to the fact that they agreed in detail on what the request had to look like, who had to issue and approve it, etc. before formalising it:

> *"And it is my- I established the relationship with […], and was sort of acting- kind of largely acting as sort of a go-between between our own Fire Service in Northern Ireland and […] that established how to go about to put the request in for the helicopters. And that information then was passed over to the Fire and Rescue Service, our own Fire and Rescue Service, and then when they needed it, they knew what to do. They didn't need to ask anybody how to go about doing it. So, it was all, I suppose, forward planning. And it was just by accident rather than design, it just came up in conversation about how I could get access to helicopters if I needed them" (ibid.).*

However formal or informal a cross-border collaborative partnership though, difficulties remain with regard to cultural, ethical and language issues. Several participants stressed that the acceptance of the tool among end-users strongly depends upon the successful incorporation of these aspects in the platform. For example, information that might be on the system for partners at one side of the border might not be at the other, because protocols to disclose this information might be different, e.g. one side might be publishing the names of victims while the other side would not.

End-users also broadly agreed that language was another important issue and, while there was an insistence that the platform should be available in different languages and be able to bridge linguistic differences, there was also a concern that the ontologies created to connect the words in different languages would become too complex to be useful. Moreover, a participant in the workshop raised awareness to the fact that a cross-border platform is only feasible if there are no disagreements regarding where the borders are located. In addition, the use of the system would have to be faster and more efficient than using current procedures in order for the platform to be adopted and accepted by the end-user organisations.

Finally, beyond acceptance by the end-users, broader societal acceptance also requires addressing politicians and the population. In this sense, communication was once again emphasised as a key factor. Once more, the ways of addressing this issue is also dependant on the cultural and organisational specifics of each country and organisation. For example, in mainland Europe, it is common for politicians to inform the public about ongoing incidents in press conferences, while in the UK that function is not fulfilled by politicians. In this context, it was emphasised that communication principles and agreements on how to involve the media before, during and after a crisis also need to be in place in collaborations in order to transmit a common picture to the public. The consistency of the message, workshop participants stressed, is critical, in order not to create panic and confusion:

> *"Public involvement was quite a big issue. So, this is a very important thing, that this is properly dealt with. Because if the wrong information is just released or just not thought about this can lead to problems. If families did not yet know that there are victims in their family and they receive the information from, through the public [media], this is not the right way. […] Wrong data to [the] press [that is] misinterpreted. […] or if the wrong information is released, this can lead to panic" (Participant, Workshop).*

Once again, training was mentioned as an important measure to help ensure good crisis communication and enhance acceptance and acceptability of the tool. However, an interviewee stated their concern that limitations to data sharing would apply with regard to simulations and decision support:

> *"For me, the support system here is in the agency […]. And here it gets all the information [simulations and decision support information] that the agency gets* [showing on a drawing that the information stays within the respective agency]. *But you will not have a decision support system in the middle. That is not allowed because nobody is allowed to get all the information and to analyse it. I think it would be fantastic if you could analyse all the information that was exchanged after a disaster, but as this is private information and the owner is the only one responsible, you can only, for the decision support system, you can only use the information that the owner has" (Research and Technology Manager, Luxembourg).*

Sharing this data raises ethical questions in terms of who is sharing the information, what happens if the information shared is wrong, who takes responsibility and pays for its development, and, once again, who owns the data, especially in case commercial providers are involved.

As a possible solution for the challenges outlined in this section, it was indicated that a combination of a top-down and a bottom-up approach for implementing the system would be best suited to enable successful inter-agency and cross-border collaboration:

> *"You have to go from both sides. If you go only from the head, the acceptance on the bottom may be missing and then you have a solution that they put on and nobody will use it, because they do not like it. On the other side, if you go only from the bottom, then nobody will pay for it (laughs)" (Research and Technology Projects Manager, Luxembourg).*

And another interviewee suggested: "it might have a lot of sense to propose HEIMDALL at national level starting from the European mechanism of civil protection. So, to share and to train people to work on the system for international emergencies" (Seismic Risks Engineer, French Geological Service, France). In sum, the right combination of providing legal and processual frameworks for cooperation and allowing space for informal communication and adaption to regional specifics, is key for fostering societal acceptance on the organisational, the political and the level of the broader public. Its acceptability thereby also relies strongly on how questions of security are addressed, and which modes of commercialisation and implementations are favoured by the business plan.

5 Conclusion and Recommendations

This deliverable has provided a summary of the work that has been carried out throughout the project to assess the societal acceptance of HEIMDALL and to evaluate and reflect upon different dimensions of ethical acceptance of such a system.

It presented an overview of the theoretical aspects of societal acceptance and ethical acceptability for HEIMDALL, which were thoroughly analysed in [6] and [7], and revised in this issue according to the deepened understanding of the tool – as one that does not interact with citizens directly – gained throughout the project as it progressed. It further outlined the methodological approach, which, in consequence of the new understanding of the tool and its acceptance, saw the initially planned focus groups with citizens replaced by a workshop involving external experts of the field of disaster management.

It has identified the significance of legal frameworks, trust, and communication for generating societal acceptance for HEIMDALL by responding to challenges to inter-organisational and cross-border cooperation in terms of the organisational, regional, cultural and linguistic differences among disaster management organisations across the EU. They should be combined with the previously identified themes [7], which include different visions of HEIMDALL, the multidisciplinary nature of the project, the commercialisation of HEIMDALL, and aspects related to decision-support, as well as data privacy and security. All of these issues were identified as both topics which are in their own relevant for societal acceptance, but at the same time intimately intertwined, so that many references were made with regard to those connections and to clarify their meaning.

It was further confirmed how the ethical acceptability of a system like HEIMDALL is influenced by cross-cutting issues related to the four dimensions introduced in section 2.2: justice, responsibility, trust, and privacy and how these interact. Hence, the importance of justice matters for usability and accessibility of the platform has been shown with respect to non-discriminatory disaster management procedures, language and cultural differences (relating to communication), as well as the commercialisation and implementation of the system. Responsibility plays an important role with regard to maintaining human autonomy and is strongly interrelated with transparency. Trust was identified not as a value per se, but as a precondition for social action, and is very influential both with regard to interaction with the platform and with other agencies. Finally, the value of privacy played a role throughout the development process in terms of “privacy by design”, adopting strong data security measures and establishing user roles and permissions.

The statements from the participants in the focus groups and workshop, the interviews devoted to identifying Human Factors for HEIMDALL and the ongoing discussions among the consortium have made clear that the societal acceptance of HEIMDALL, as a platform that does not interact with the broader public as such, relies very much on these contextual conditions which provide the framework for its acceptance. The challenge and opportunity lie in providing the structures for its implementation (top-down), and thereby reducing bureaucratic efforts and speeding up operational procedures, while at the same time allowing for adaption of the tool to the needs and regional specifics of each organisation (bottom-up).

In terms of recommendations which could be made based on this analysis, several points to consider emerged. The overall objective of HEIMDALL, that is to help saving lives and reducing damage in crisis situations, was supported by all of the participants in the interviews, focus groups and workshop. Opportunities to provide support to disaster managers throughout preparedness, response and recovery phases of a disaster are abundant, as many statements by end-users and other experts confirmed throughout this research. What is more, the system yields potential to strengthen cooperation and standardisation of crisis response in the European Union. However, as presented in this issue, important concerns prevail with regard to its acceptance and acceptability, which should be considered if moving to the commercialisation phase.

Firstly, as already outlined in [7], different visions of the system prevail between different types of end-users, technical developers and data providers. On the one hand, complex decision-support modules are designed in a fashion ultimately aimed at a system which provides concrete suggestions for decisions, while on the other hand, the end-users emphasised unequivocally that they did not want the tool to decide for them, as they wish to retain their autonomy and responsibility drawing on their expertise and experience. They would rather see the platform as a tool to gather and filter data, but C&C were seen as the managers of the system. In the field, the system would be used mainly for communication. Beyond that, many end-users mentioned that the system could also be an asset for training. These different visions of the tool and different understandings of its functionalities were also present in the consortium discussions, reflected in different terminologies and mental models. Ensuring acceptance of the system by the end-users, as well as its acceptability, implies bridging this understanding gap between technical profiles and end-user profiles. While much conversation and progress has been done in this respect, this challenge will continue in the sense that the system will encounter different end-user organisations and contexts if implemented.

Secondly, as stressed in both [7] and sections 2.2 and 4.2, trust has been identified as one of the key factors for the acceptance of the system. This is related both to interpersonal trust, and trust in the data the system provides. Achieving a balance between providing valuable data, filtering information and offering best options without influencing a decision is vital for an ethically acceptable system. In this sense, HEIMDALL should support current responsibilities structures and improve the cooperation among first responder organisations.

Matters of trust and responsibility have shown important particularly with regard to the decision support functionalities [7]. Therefore, in order to enhance quality, veracity and confidence in the data HEIMDALL provides, transparency should be ensured, for example, by indicating the source of the data, the parameters involved in decision support and the weights given to them. In this sense, answering the questions related to the ownership and use of the data as well as the actions taken to avoid a potential function creep are vital points for societal acceptance and to hinder the generation/reinforcement of injustices.

Connected to the previous point, in the disaster management field trust is based on the face-to-face interaction and previous experiences of working together. The empirical results presented in this deliverable add further merit to the importance of communication both among disaster managers and with the public. Developing a system that adds value to this cooperation via better communication tools, sharing of the operational picture, and distribution of data and lessons learnt could be key elements to secure the societal acceptance of HEIMDALL. Also, considering the rising importance of social media as a medium for people to communicate and connect in crisis situations, HEIMDALL can function as a tool to enhance disaster communication and provide assistance and assurance to the population and thereby generate direct acceptance in the community.

Furthermore, as HEIMDALL aims to both support and connect existing structures and add new features to enhance disaster management processes, the topic of interoperability has proved a key challenge to overcome in order for the tool to provide added value, especially in the context of cross-border cooperation. Section 4.4 has highlighted that there is a trade-off between legal frameworks and formalised agreements which provide the context within which collaboration can take place and interpersonal contact and informal communication required to make such collaboration work. Such trade-offs take place in distinctive regional and socio-cultural contexts, where the system is applied. In this sense, the acceptance of the tool depends upon both its usability given the respective regulatory framework and its ability to accommodate specific needs and characteristics of the particular context. Therefore, a balanced combination of top-down and bottom-up implementation of the tool has been suggested.

Another recurring concern revolved around security and the respective measures that HEIMDALL should adopt in terms of roles and access levels as well as related to guarantee that no data breaches and/or potential misuses of the data may happen that, as previously mentioned,

create/reinforce injustices. This point was elaborated in detail in [7], but since it is connected to other issues such as trust and cooperation, especially with regard to data sharing, references have been made to this point accordingly.

Finally, many of the concerns about acceptance and acceptability of the system depend upon its commercialisation, as explicated in [7], but also touched upon with regard to Human Factors in [5]. As stated in this issue, many of the mentioned issues are to some degree related to this matter, as concerns were repeatedly raised about who owns the data shared and who would be responsible in case of leaks or breaches. Furthermore, it is a concern in terms of affordability and justice, for example who carries the costs for acquiring the system if other, similar systems are already in place, and moreover, which areas are deprived of funding for the sake of acquiring HEIMDALL. In other words, what are the costs of acquiring HEIMDALL for an organisation? and are they outweighed by the benefits for crisis management? These questions need to be considered in order to render the system socially and ethically acceptable. Therefore, the business plan should take into consideration the multiple interests and objectives of the project partners as well as economic and environmental differences among EU countries.

In sum, this final issue of the series of deliverables on societal acceptance and ethical acceptability has shown that ethical and social challenges which were identified throughout the project have been continuously addressed, while new ethical issues and socio-cultural and legal issues will continue to emerge when the system moves from the prototype stage to its implementation at specific organisations and places. These socio-cultural and legal concerns are, of course, beyond the technical solutions the system can provide at this stage and will require the continuous adaption from both HEIMDALL and the respective organisations adopting it. In this sense its contribution to the overall crisis management of the corresponding area will depend upon these contextual conditions and the mutual adaption required to address them.

6 References

[1] Regina Ammicht Quinn: „Sicherheitsethik. Eine Einführung“ (2014). In Regina Ammicht Quinn (ed.): Sicherheitsethik. Wiesbaden: Springer VS (Studien zur Inneren Sicherheit, 16): 15–47.

[2] Gerhard Chroust: “Social Media in Crisis Situations” (2013). In Doucek, P.; Chroust, G.; Oskrdal, V. (eds): Information Technology, Human Values, Innovation and Economy. Linz: Trauner Verlag: 13-22.

[3] HEIMDALL Deliverable D3.8: Analysis of Human Factor Involvement in the use of Autonomous Systems in DRR and Response and Specifications for User Requirements – Issue 1.

[4] HEIMDALL Deliverable D3.9: Analysis of Human Factor Involvement in the use of Autonomous Systems in DRR and Response and Specifications for User Requirements – Issue 2.

[5] HEIMDALL Deliverable D3.10: Analysis of Human Factor Involvement in the use of Autonomous Systems in DRR and Response and Specifications for User Requirements – Issue 3.

[6] HEIMDALL Deliverable D3.11: Analysis of Societal Acceptance and Ethical Acceptability – Issue 1.

[7] HEIMDALL Deliverable D3.12: Analysis of Societal Acceptance and Ethical Acceptability – Issue 2.

[8] Armany Elbanna, Deborah Bunker, Linda Levine, and Anthony Sleigh: “Emergency Management in the Changing World of Social Media: Framing the T Research Agenda with the Stakeholders through Engaged Scholarship” (2019). International Journal of Information Management 47: 112-120.

[9] Martin Endreß and Benjamin Rampp: „Vertrauen in der Sicherheitsgesellschaft“ (2013). In Sitzungsberichte: Technik - Sicherheit - Techniksicherheit. 5. Symposium des Arbeitskreises Allgemeine Technologie. Leibniz-Sozietät der Wissenschaften zu Berlin und Institut für Technikfolgenabschätzung und Systemanalyse des Karlruher Instituts für Technologie, edited by Gerhard Banse und Ernst-Otto Reher. Berlin (116): 145–160.

[10] Markus Enenkel, Sofía Martinez Sáenz, Denyse S. Dookie, Lisette Braman, Nick Obradovich, Yury Kryvasheyeu: “Social Media Data Analysis and Feedback for Advanced Disaster Risk Management” (2018). ArXiv:1802.02631.

[11] Ali Farazmand: “Crisis and emergency management: Theory and practice. Crisis and Emergency Management” (2014). Routledge: 25-34

[12] Alexis Gizikis, Tony O’Brien, Iratxe Gomez Susaeta, Matthias Habdan, Annika Schubert, Christian Reuter, Marc-Andre Kaufman, Joe Cullen, Andrew Muddiman, Mattia Perruzza, Uberto Delprato: “Guidelines to increase the benefit of social media in emergencies” (2017. EmerGent: Emergency Management in Social Media Generation, deliverable 7.3.

[13] In-Prep: “What is In-Prep?” (2017) Available at: https://www.in-prep.eu/ [last checked: 10.11.2020].

[14] Siegfried Lamnek: „Gruppendiskussion“ (2005): Theorie und Praxis. Weinheim: Beltz.

[15] Michael McGuire and Chris Silvia: “The effect of problem severity, managerial and organizational capacity, and agency structure on intergovernmental collaboration: Evidence from local emergency management” (2010). Public Administration Review 70: 279-288.

[16] Rune Ottosen, Stehen Steenson: “Blood and Security during the Norway attacks: Authorities´ Twitter activity and silence” (2018) In: Harald Hornmoen, Klas Backholm (eds.): Social Media Use in Crisis and Risk Communications: Emergencies, concerns and awareness. Bingley, UK: Emerald Publishing: 63-84.

[17] Nitin Pangarkar: “A framework for effective crisis response” (2016). Journal of Organizational Change Management 29: 464-483.

[18] Katrina Petersen, Monika Büscher, Maike Kuhnert, Steffen Schneider and Jens Pottebaum: “Designing with Users: Co-Design for Innovation in Emergency Technologies” (2015). Short-Paper - Ethical, Legal, Social Issues; Proceedings of the ISCRAM 2015 Conference, Kristiansand May 24-27.

[19] Christian Reuter, Thomas Ludwig, Macr-André Kaufhold and Thomas Spielhofer: “Emergency services´ attitudes towards social media: A quantitative and qualitative survey across Europe” (2015). International Journal on Human-Computer Studies 95: 96-111.

[20] Florian Roth and Tim Prior, Tim: “Utility of Virtual Operations Support Teams: an international survey” (2019). Australian Journal of Emergency Management 34(2): 53-59.

[21] Simon Tomer, Avishay Goldberg and Bruria Adini: “Socializing in Emergencies – A review of the use of social media in emergency situations” (2015), International Journal of Information Management 35: 609-619.

[22] United Nations Office for Disaster Risk Reduction: “Sendai Framework for Disaster Risk Reduction 2015-2030” (2015). Available at: https://www.unisdr.org/files/43291_sendaiframeworkfordrren.pdf [last checked July 2017].

[23] Paul Upham, Christian Oltra and Álex Boso: “Towards a cross-paradigmatic framework of the social acceptance of energy systems” (2015). Energy Research & Social Science 8:100-112.

[24] Andreas Wolkenstein: “Akzeptanz und Akzeptabilität im Kontext der Angewandten Ethik.” (2014) In Regina Ammicht Quinn (ed.): Sicherheitsethik. Wiesbaden: Springer VS (Studien zur Inneren Sicherheit, 16): 225–239.

End of document