D8.5
POPD - Requirement No. 8

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	42 months
Contributing WP	WP8
Dissemination Level	CO
Contractual Delivery Date	M12
Actual Delivery Date	30/04/2018
Editor	Andreas Baur (EKUT)
Contributors	Prof. Dr Regina Ammicht Quinn, Andreas Baur, Dr des. Anne Burkhardt, Friedrich Gabel, Solange Martínez Demarco (EKUT)

Document History			
Version	Date	Modifications	Source
0.1	12/03/2018	First draft.	EKUT
0.2	27/03/2018	Implementation of partners' responses.	EKUT
0.3	06/04/2018	Second draft.	EKUT
0.3	13/04/2018	Ready for quality assurance review.	EKUT
0.4	24/04/2018	QA reviewed version	DLR
1.0.F	27/04/2018	Final version.	EKUT

Table of Contents

List of Tables

List of Acronyms

AVA	Avanti Communications LTD
CIMA	Centro Internazionale in Monitoraggio Ambientale – Fondazione CIMA
CTTC	Centre Tecnològic de Telecomunicacions de Catalunya
DLR	Deutsches Zentrum für Luft- und Raumfahrt e.V.
DLR-DFD	Deutsches Zentrum für Luft- und Raumfahrt e.V.; German Remote Sensing Data Center.
DLR-KN	Deutsches Zentrum für Luft- und Raumfahrt e.V.; Institute of Communications and Navigation
DLR-KN-COS	Deutsches Zentrum für Luft- und Raumfahrt e.V.; Institute of Communications and Navigation; Department of Communication Systems
EU	European Union
EKUT	Eberhard Karls Universität Tübingen
GB-SAR	Ground based synthetic aperture radar
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
GPS	Global Positioning System
ICGC	Cartographic and Geological Institute of Catalonia
ID	Identifier
ISA	Impact Summary
MAVs	Micro Aerial Vehicles
PbD	Privacy by design
PCF	Fundació d'Ecologia del Foc i Gestió d'Incendis Pau Costa Alcubierre
PET	Privacy Enhancing Technologies
POPD	Privacy or protection of data
REA	Research Executive Agency
R&D	Research and Development
RVA	Risk and Vulnerability
SPH	Space Hellas S.A.
TSYL	Tecnosylva S.L.
UNISTRA	Université de Strasbourg
URL	Uniform Resource Locator
VPN	Virtual Private Network

WP	Work Package
ZENDAS	Zentrale Datenschutzstelle der baden-württembergischen Universitäten

Intentionally blank

Executive Summary

This deliverable presents the procedures and efforts pursued by the HEIMDALL consortium ensuring that no privacy or data protection requirements are being transgressed during research and development (R&D) activities of HEIMDALL.

It shows also, how principles and strategies of privacy by design are taken into account for the design and functioning of the HEIMDALL system.

This deliverable answers to the following requirement identified in the Ethics Summary Report: POPD - Requirement No. 7.

1 Introduction

The POPD Requirement No. 7 asked to give ‘detailed information […] provided on the procedures that will be implemented for data collection, storage, protection, retention and destruction and confirmation that they comply with national and EU legislation. With the project's new data management policy involving tracking of persons and surveillance (even of project participants), a “privacy by design” procedure must be detailed and presented to the REA.’

This document will answer to this requirement. Firstly, it summarises in section 2 the definition of personal data provided by the EU General Data Protection Regulation, the necessity of privacy by design, the background of the concept and specific principles and strategies. Section 3 presents how HEIMDALL partners keep the processing of personal data for their research and development activities to the lowest possible level. Furthermore, tasks that need to process personal data for research and demonstration are reported and the procedures for collection and data protection are detailed as well as the legal compliance of these procedures. This is followed by an overview of how privacy by design strategies are taken into account in the design of the HEIMDALL system.

.

2 Personal Data and Privacy by Design

2.1 GDPR Definition of Personal Data

Within the new General Data Protection Regulation (GDPR) [1] that was recently adopted by the European Union, came into force and will be fully applicable beginning in 25 May 2018, article 4 provides a series of definitions among which the following ones are useful for HEIMDALL development, and particularly, this deliverable.

Personal Data is understood as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

In addition, the same article proposes to understand processing as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

With regards to pseudonymisation as a method for processing personal data, it “means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.

Finally, in order to process personal data, a consent must be given. In this sense, “‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

2.2 Why Privacy by Design?

The notion of privacy by design (PbD) goes back to John Borking who presented in 1995 his ideas of Privacy Enhancing Technologies (PET). Based on the fact that during the Second World War, already existing lists of Dutch inhabitants indicating their religion helped the Nazis to prosecute Jews in occupied Netherlands, he issued his strong opinion that technology should never again help to commit such crimes. Therefore, he argued for privacy enhancing technologies that can guarantee that only necessary data is processed and the privacy and dignity of humans can be protected.

Furthermore, Ann Cavoukian, the then Canadian Information & Privacy Commissioner, published the concept of privacy by design in the 1990s and thereby extended the idea of privacy enhancing technologies to include positive values. She formulated seven foundational principles of privacy by design that should be followed not only in the development of technology, but also in the organisation of businesses and systematic practices. She argues: ‘Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization’s default mode of operation’ [1].

Thereby, a system should be designed in a way that keeps the following sentence in mind: ‘Do not trust anyone, including yourself.’ Nobody should trust him- or herself that he/she will act in a crisis situation according to moral or legal standards and that one can assess the functioning and security of a system only by oneself.

But privacy by design is not only a scientific or ethical concept, it has also become a very important part of the EU’s regulatory framework. With the new General Data Protection Regulation (GDPR), privacy by design has become one of the core values that developers of

technology, businesses and organisations have to implement and adhere to. In the following, the relevant article of the GDPR is cited (emph. added):

‘Article 25 (GDPR): Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, **the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as *pseudonymisation*, which are designed to implement data-protection principles, such as *data minimisation*, in an effective manner and to integrate the necessary *safeguards* into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.**
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, **only personal data which are necessary for each specific purpose of the processing are processed**. **That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.** In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.’

2.3 Foundational Principles of PbD

In the following, the seven foundational principles of privacy by design are shortly summarised (see also [1]):

1. *Proactive not Reactive; Preventative not Remedial*

   Anticipate and prevent privacy violations and do not wait for privacy risks to materialise or resolve them after they have occurred. Privacy by design comes before-the-fact, not after.

2. *Privacy as the Default*

   Privacy is the default setting so that if an individual does nothing, their privacy is still automatically protected and no action by users is required as privacy is already ‘turned on’.

3. *Privacy Embedded into Design*

   Privacy is embedded in the design and architecture of the system and the practices. Privacy is integral to the core functioning and not only an add-on or a limitation to the functionality.

4. *Full Functionality – Positive-Sum, not Zero-Sum*

   Privacy and other legitimate interests and objectives (such as security) are not contrary or a trade-off. Privacy by design avoids false dichotomies and shows a win-win or positive-sum result, for example demonstrating that both privacy and security can be achieved.

5. *End-to-End Security – Full Lifecycle Protection*

   Privacy by design is embedded into the system before the first information is being processed and covers the whole lifecycle of the information. Strong security is important from start to finish. All data is securely collected, retained and also destroyed shortly after the end of the process.

6. *Visibility and Transparency – Accountability, Openness, Compliance*

   Assure all users and stakeholders that the system is working according to the stated promises and objectives. Make independent verification possible by keeping all components and processes visible and transparent.

7. *Respect for User Privacy – Consent, Accuracy, Access, Compliance*

   Respect the interest of the individual uppermost. Keep it user-centric, make privacy the default, notice the individual when needed and empower user-friendly options.

2.4 Privacy Design Strategies

Eight privacy design strategies following Jaap-Henk Hoepman (2014) [5]:

1. MINIMISE

   Restrict data collection and processing to the least amount possible. Ask yourself whether the data is necessary, whether its collection is proportional in relation to the expected purpose and whether there is no less invasive means to achieve the same purpose. A common design pattern reflecting this strategy is called ‘select before you collect’.

2. HIDE

   Any personal data and their interrelationship should be hidden from plain view. This helps to hinder abuse of the information. This strategy helps to ensure confidentiality and the specification of from whom the information should be shielded. This depends on the context. It also helps to achieve *unlinkability* and *unobservability*.

3. SEPARATE

   Personal data should be processed in a distributed and decentralised way. This ensures the impossibility to create complete profiles of persons. Data from different sources should be stored separately and locally. This helps also to achieve the purpose of limitation.

4. AGGREGATE

   Personal data should be processed with the highest possible level of aggregation. This includes that the processed data contains the least possible level of detail but is still useful. Sensitive information thereby becomes less sensitive if the groups and aggregation level is high enough. This information therefore cannot be attributed to a single individual. A useful design pattern is depersonalisation/anonymisation.

5. INFORM

   Every time an individual uses a data processing system, the user should be informed about what data is processed, for what purpose and how. And also, how it is protected and who has access to this information. Moreover, data subjects should be provided with information about their access and deletion rights. This helps to ensure openness and transparency.

6. CONTROL

   This strategy is an important counterpart of the INFORM strategy. Data subjects should be provided agency and control over the processing of their personal information. If individuals do not have an influence on the processing of their data, there is no sense in informing them about the processing in the first place. And vice versa: If data subjects are not informed about the processing of their data, there is no sense in giving them the right to intervene in these processes. Design patterns like user centric identity management and end-to-end encryption can be part of the CONTROL strategy.

7. ENFORCE

There should be a privacy policy in place that is compatible with legal requirements and this privacy policy should be enforced.

8. DEMONSTRATE

   There should be a data controller who is able to prove compliance of the system with the privacy policy. This strategy is also important to provide transparency. The use of logging and auditing can help to implement this strategy.

3 Efforts of the Consortium in order to ensure minimal use of Personal Data and Privacy by Design

3.1 Minimal Use of Personal Data

EKUT provided the GDPR definition of personal data and informed all project partners of the HEIMDALL consortium about the necessity to process personal data according to the respective legal framework.

In return, the following partners stated that they will not gather or process personal data during the research and development activities of the HEIMDALL project: AVA, CIMA, CTTC, DLR-DFD, DLR-DFD-COS, DLR-KN, ICGC, PCF, SPH, TSYL, UNISTRA.

As it has been identified that specific personal data is necessary during the activities related to Users and Roles Management and Crowdsourced and First Responders Data modules, the agreement has been to create mock-up user accounts for testing purposes. In this way, testing the login/logout functionality, the role management feature and the location information of first responders will not identify 'real' individuals. In addition, EKUT will keep to the minimum the gathering and processing of personal data that is necessary for its research activities related to social and ethical acceptability as well as human factors.

In the following, the measures taken to protect this data are outlined.

3.1.1 Gathering and Processing of Personal Data during Research Activities

In work package 3, as reported by PCF, the collection of the necessary case studies, lessons learnt and best practices to populate the repository of scenarios to be used during the test case will not entail the gathering of personal data. The focus of this task (3.3) will be on the process, the circumstances, and the results of the intervention of the first responders in the emergency, and will not identify any person that has provided the information. The type of data to be gathered includes photos of the incident, cartography, hazard data, behaviour analysis, incident organisation, and derived lessons learnt and best practices.

However, during the research activities in work package 3, EKUT is collecting personal data in task 3.4 which are needed for the research on social acceptance and ethical acceptability as well as human factors. The personal data comprise audio files of focus group discussions and interviews as well as a list of (possible) interviewees stating name, information on the professional background such as occupation and affiliation, and professional contact details.

The audio files of the focus group discussions are transcribed and thereby anonymised (no names or organisations are noted) and directly deleted afterwards. Interviews are transcribed and the names deleted if asked for by the interviewees. All participants are informed about the research, the collected data and its processing and usage through the project information sheet, and show their consent by signing consent forms. These files can be found in D8.2, with the notable addendum that audio files of focus group discussions will be deleted right after the transcription. The gathering and deletion procedures ensure that only necessary data is being stored for as short as possible.

This procedure is reported in detail in the 'Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO' (translates to: register file on data processing of the responsible person according to Art. 30 par. 1 GDPR) from 26 April 2018. This is required under the data protection regulation of the *Zentrale Datenschutzstelle der baden-württembergischen Universitäten- ZENDAS* (Central data protection body of the universities in the state of Baden-Württemberg, Germany). The collection and storage of personal data by EKUT thereby complies with the new General Data Protection Regulation (GDPR) (EU) 2016/679 and the Landesdatenschutzgesetz Baden-Württemberg [3] [6] (state laws on data protection). The register file is attached to this deliverable.

By applying this procedure, EKUT furthermore implements several privacy by design strategies: MINIMISE (only the information needed), HIDE (encryption and authentication measures), AGGREGATE (transcripts are anonymised), INFORM (being transparent about the data processing before the collection), and CONTROL (participants have always the right to withdraw).

3.1.2 Gathering and Processing of Personal Data during Demonstration Activities

During the demonstration activities, as far as it is foreseeable at this point in time, some tasks require the processing of personal data by some partners. All partners are aware of the sensitivity that comes with the processing of personal data and will keep the collection and processing of personal data to the lowest possible level. This is also shown in the several ways the HEIMDALL consortium is implementing privacy-by-design principles and strategies in the system they are developing.

Most of the data used is mock-up data or test data that is not personal. However, during the demonstration phase, user ID, password and smartphone GPS coordinates will be required. In order to legally gather these data, the participants of the exercise will be provided with oral and written information about the project, the privacy policy and a consent form that should be signed to manifest agreement. The option to share the location of the user with other HEIMDALL modules and with users from different entities by default will be deselected, which is the only information requested, complying with the MINIMISE strategy. In no case, the Service Platform, the module orchestrating the functioning of the platform, will share the location of a person to modules outside of HEIMDALL, or to modules that should not use the location of the user, following the HIDE strategy.

Below there is an explanation, provided by AVA, of how personal data will be processed during the actual pilot test that will be undertaken with users as part of the project. It shows the efforts of the consortium to minimise the gathering and processing of personal data during the demonstrations.

Table 3-1: Personal data to be processed during the demonstration case and PbD principles adopted

#	Personal data to be processed	Processing of personal data in accordance with privacy by design principles
1	Login information - user ID and password.	• Only pre-approved/authorised users who are members of the HEIMDALL consortium will be provided with suitably anonymised login credentials. • Communication of the anonymised login credentials entered by the user will be encrypted and/or sent via a secure channel to the applicable HEIMDALL back-end service. • Users will be logged out automatically after a period [to be defined] of inactivity.
2	User location information - from smartphone GPS coordinates.	• Only the location of pre-approved/authorised users who are members of the HEIMDALL consortium and who would have consented to the information being used for the purposes of the project will be processed. • The user location information will be encrypted and/or sent via a secure channel to the applicable HEIMDALL back-end service. • The location information will be suitably anonymised before being presented to the consortium or documented.

Participants in the demonstration will be informed about what kind of data is collected and processed and for how long. Only members of the HEIMDALL consortium who have voluntarily expressed their consent to the processing of personal data will participate in the demonstrations.

The following partners will, according to the current development plan, process personal data and take care of the informed consent forms and the respective legal requirements of data protection:

- DLR-KN, SPH and AVA for the creation of demo accounts used by participants and the possibility to share location data to other HEIMDALL demonstration participants. DLR-KN is checking with their legal department before the testing and demonstration activities what documentation is needed in order to comply with regional and European data protection regulation.
- In order to provide data for landslides, CTTC plans to use video cameras and to store the recorded videos during demonstration activities. Although the cameras will be installed in abandoned areas, people might still be captured by them. CTTC will put signs indicating the active webcam, the data processor (CTTC/HEIMDALL), the goals of the projects (the not-for-profit and public utility characteristics of the project) (INFORM strategy), and the rights of the individual/person (CONTROL strategy). In this sense, if people get filmed, the recorded video will be blurred as a default practice (complying with the INFORM, CONTROL, HIDE and MINISE strategies). Moreover, the real-time and stored images will be accessible only to strictly authenticated and authorised CTTC/HEIMDALL users. CTTC is contacting the respective data protection authorities in order to make sure that the video recording is complying with data protection regulations in place.

These partners will keep the consortium updated on the processing of personal data and the necessary steps to comply with the regional data protection regulations. Most of the regional and national data protection regulations have to be adjusted to the EU General Data Protection Regulation. Only some member states of the European Union have already finished this adoption process. This leads to delays in the processes of verifying compliance.

3.2 The Privacy-by-design Implementations into the HEIMDALL System

The partners within the HEIMDALL consortium have been provided with background information on the necessity of privacy by design when it comes to the processing of personal data. The ways of implementing the privacy-by-design strategies were evaluated in the discussions afterwards. In the following, the focus lays on the results of analysing the applicability of implementing PbD into the system under development (in contrast to the personal data needed for research and development as reported in section 3.1).

Examples of the application and implementation of privacy-by-design principles and strategies are reported below, summarised along the work packages of the system development.

3.2.1 **Work Package 4: Platform Services**

The partners responsible for the development and design of the platform services reported the following implementation of PbD strategies and principles in the HEIMDALL system.

As in the case of the demonstration activities, the option to share the location of the user with other HEIMDALL modules and with users from different entities by default will be deselected, which is the only information requested, complying with the MINIMISE strategy. In no case, the location of a person will be shared to modules outside of HEIMDALL by the Service Platform, the module orchestrating the functioning of the platform, or to modules that should not use the location of the user, following the HIDE strategy.

Furthermore, the user accounts database will be different from the database that stores georeferenced information (which will also collect other georeferenced data such as images of the incident, shared by the users), implementing the SEPARATE strategy. As such, this strategy will comply with purpose limitation and reduce the options to produce a complete profile.

The user accounts will remain private, as well as the data/products the users generate. The users will have the freedom to choose with whom to share which data/products generated by using the HEIMDALL system. As a platform with a user centric design, the user will always keep control of their data and/or products.

The privacy policy will state the same for rest of the modules that capture and/or use the user location and/or user accounts, adopting the respect for user privacy and visibility and transparency principles. This comprehensive INFORM strategy will show all users and stakeholders the objectives of the system, identify the data controller, the type of data collected, the purposes and uses, and whether any of this information will be disclosed and the measures taken (practices and procedures) for security.

Through the access control functionality of the Users and Roles Management module security will be imposed to the system. Communication among HEIMDALL components (data transfers) will be performed through secure VPN connections ensuring an end-to-end security, thereby complying with the CONTROL strategy. In addition, the Service Platform monitoring module will keep track of the status of modules and which components and processes are active. Logging will be used to keep a register of this, and thereby implements the DEMONSTRATE strategy.

3.2.2 **Work Package 5: Existing Data Sources and Services**

The partners responsible for the development and design of the integration of existing data sources and services reported the following implementation of PbD strategies and principles in the HEIMDALL system.

The use of Micro Aerial Vehicles (MAVs) swarm for early detection of forest fires and landslides will not entail the collection of personal data. Video footage of the regions of interest will be transmitted in real time to a base station and never stored (MINIMISE strategy).

Ground based synthetic aperture radar (GB-SAR) is the selected type of in situ sensors for detecting landslides. They will be installed in a private area specifically requesting the permission for this to the owner of the land. The data/information acquired by radar consists of digital number not associable to any human feature.

Currently, CTTC is in contact with the corresponding data protection authority to learn about the best strategy for carrying out this activity which also includes installing and using video cameras adopting the necessary PbD measures. The partner will keep the consortium informed about the results.

3.2.3 **Work Package 6: Assessment and Decision Support Services**

The partners responsible for the development and design of the assessment and decision support services reported the following implementation of PbD strategies and principles in the HEIMDALL system.

The privacy of individual end users will be protected by using authorisation and authentication methods based on user profiles connected to groups and not to individual accounts, which complies with the MINIMISE and HIDE strategies. In addition, User and Roles Management will be managed centralised and project-wide and applied by all HEIMDALL modules (CONTROL strategy).

Furthermore, the necessary computations carried out as part of this work package will rely on expert criteria and census data. The “affected people” or “potential people at risk” is the result of an analysis carried out at building level that will consider the ‘total number of people present/resident in the building’ and the ‘percentage of vulnerable classes of people’, and as such will only use information at population level. In other words, as a product of task 6.3 will implement the AGGREGATE strategy, providing a number of people as a whole without reflecting any specific individuals.

Also, the data for these computations will reside in different HEIMDALL modules. For example, human impact assessment information provided by the Risk and Vulnerability (RVA) module (task 6.2) will be used in the Impact Summary (ISA) module (task 6.3) for the generation of “people at risk” numbers which in turn will be used by the Situation Reporting module which will reside next to the Scenario Management module, applying the separate principle. Through the strong modularization of the HEIMDALL system data resides in the respective modules which generate that data and is referred to by reference (e.g. URL) and not duplicated.

Additionally, the users will be INFORMed of the configuration options of these modules by readme files and instructions.

4 Conclusion

This deliverable provided the GDPR definition of personal data as well as information regarding privacy by design background, principles and strategies. This information was provided and discussed with all the partners of the HEIMDALL consortium in order to evaluate the activities that are carried out during the R&D phase, as well as the final design of the system.

The assessment determined that only minimum personal data is necessary for research, testing and demonstration activities, as well as for the design of the system. The strategies and actions that are implemented to enforce privacy by design were detailed. In addition, this deliverable stated the procedures adopted for data collection, storage, protection, retention and destruction of personal data.

Currently, the partners mentioned in 3.1.2 are in contact with the respective regional data protection authorities in order to obtain confirmation that these approaches are complying with the corresponding national and EU legislation.

5 References

[1] Cavoukian, A., Taylor, S., Abrams, M.E. (2010) “Privacy by Design: essential for organizational accountability and strong business practices”, Identity in the Information Society 2(3), 405-413.

[2] General Data Protection Regulation (EU) 2016/679.

[3] Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 (Baden-Württemberg).

[4] HEIMDALL Deliverable D8.2: “H – Requirements No. 5”, July 2017

[5] Hoepman, J. H. (2014) “Privacy Design Strategies”, in: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam A., Sans T. (eds) *ICT Systems Security and Privacy Protection*. *SEC 2014. IFIP Advances in Information and Communication Technology*, vol 428. Berlin/ Heidelberg: Springer.

[6] Landesdatenschutzgesetz Baden-Württemberg: Gesetz zum Schutz personenbezogener Daten in der Fassung vom 18. September 2000.

Annex A. Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO

See the following pages.

End of document

Verzeichnis von Verarbeitungstätigkeiten

des Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO

- Besonderer Teil * -

Datum	26.04.2018	Az. (intern)

☒ Neue Verarbeitungstätigkeit

☐ Änderung bestehender Verarbeitungstätigkeit

1 Bezeichnung der Verarbeitungstätigkeit[1]

Bezeichnung der Verarbeitungstätigkeit	Fokusgruppendiskussionen und Interviews, Forschungsprojekt HEIMDALL
Zweck der Verarbeitung	Erhebung von empirischen Daten zu Fragen der sozialen Akzeptanz der Projektentwicklungsergebnisse

2 Innerorganisatorische Ansprechpartner[2]

Verantwortliche Fachabteilung	Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
Fachlicher Ansprechpartner	Prof. Dr. Regina Ammicht Quinn
Telefon	+49 7071 29-77983
E-Mail-Adresse	regina.ammicht-quinn@uni-tuebingen.de
Technischer Ansprechpartner	Andreas Baur
Telefon	+49 7071 29-77988
E-Mail-Adresse	a.baur@uni-tuebingen.de

3 Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen[1]

Name	
Straße	
PLZ, Ort	
Land	

* [1,2] Hinweis: Bei Angaben, die im Folgenden mit ([1]) gekennzeichnet sind, handelt es sich um solche, die gemäß Art. 30 DS-GVO zwingender Bestandteil des VVT sein müssen. Angaben, die im Folgenden mit ([2]) gekennzeichnet sind, sind solche, die aus Gründen der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO notwendig sind. Weitere Informationen dazu finden Sie in unseren Ausfüllhinweisen.

Telefon

E-Mail-Adresse

4 Beschreibung der Verarbeitungstätigkeit[2]

Das EU-Horizon2020-Projekt HEIMDALL zielt darauf ab, die Fähigkeit von Gesellschaften zur Bewältigung komplexer Krisensituationen zu verbessern. Dazu sollen integrierte Werkzeuge zur Verfügung gestellt werden, die eine effiziente Reaktion ermöglichen und durch die Erstellung realistischer multidisziplinärer Szenarien auch die Planung und Vorsorge unterstützen. Das im Rahmen des Projekts zu entwickelnde System dient dabei der Unterstützung und Erleichterung der organisatorischen Koordinierung und dem Datenaustausch zwischen vielen Akteuren (Feuerwehreinheiten, medizinische Notdienste, Polizeidienststellen, Katastrophenschutzeinheiten, Kommando- und Kontrollzentren).

Das Ethikzentrum wird in Zusammenarbeit mit den am Projekt beteiligten Endnutzern eine Analyse der menschlichen Faktoren, der gesellschaftlichen Akzeptanz und der ethischen Akzeptabilität sowie eine Analyse der ethischen Fragen durchführen. Hierzu führen Mitarbeiter_innen des IZEW zum einen Fokusgruppendiskussionen durch. Diese werden aufgezeichnet (ca. 5x60 Minuten mit jeweils 6–9 Projektpartnern oder freiwilligen Externen), Namen oder Institutionen werden aber nicht notiert. Zum anderen werden ca. 24 Interviews durchgeführt, die ebenfalls aufgezeichnet und transkribiert werden.

Zur Vorbereitung der Interviews und der Diskussionen mit Externen werden mögliche Interviewpartner_innen gesucht und angefragt, hierzu werden wenige personenbezogene Daten wie Namen, Arbeitsbereich und Expertise, Institutions- oder Unternehmenszugehörigkeit notiert.

Die Datenerhebung in den Diskussionen und Interviews selbst laufen wie folgt ab: Partner und Freiwillige werden über Inhalt und Zweck der Projektarbeit und der Interviews/Diskussionen informiert. Dazu wird auch ein *project information sheet* ausgegeben. Auf einem *consent form* werden alle Informationen zur Datenverarbeitung aufgeführt und auf die Rechte der Teilnehmenden und die Freiwilligkeit der Teilnahme verwiesen. Außerdem wird mündlich auf die Freiwilligkeit der Teilnahme hingewiesen und betont, dass eine Nicht-Teilnahme keinerlei negative Konsequenzen nach sich zieht. Hierdurch wird eine Drucksituation vermieden. Die Teilnehmenden werden gebeten – wenn keine offenen Fragen mehr bestehen – das *consent form* vor der Teilnahme zu unterschreiben, um ihre Teilnahmebereitschaft zu bestätigen. Auch nach der Durchführung der Interviews ist ein Austritt/Rückzug möglich. Bei Interviews zieht dies die Löschung der Audio-Datei und des Transkripts nach sich, bei Fokusgruppendiskussionen die Löschung der dieser Person zugeordneten Sätze aus dem Transkript. Anschließend werden die Audiodateien transkribiert (ohne Identifikation der Diskutierenden) und die Audiodateien gelöscht. Bei Fokusgruppendiskussionen ist somit im Anschluss an die Transkription kein Personenbezug mehr möglich. Bei den Interviews wird zur besseren Auswertbarkeit und Einordnung der Name und die Funktion des/der Interviewten auch im Transkript notiert, es sei denn, der/die Interviewte möchte das nicht. Die Transkripte werden IZEW-intern verwendet und nicht veröffentlicht, lediglich anonymisierte Zitate sowohl aus den Interviews als auch den Diskussionen können in Publikationen verwendet werden.

5 Kategorien personenbezogener Daten[1]

In der Spalte Bes. ist ein „x“ zu setzen, wenn das jeweilige Datum einer besonderen Kategorie personenbezogener Daten gemäß Art. 9 DS-GVO oder Art. 10 DS-GVO zuzuordnen ist.

Lfd. Nr	Beschreibung	Bes.
1	Tondateien der Fokusgruppendiskussionen ohne Namensnennung	–
2	Namen möglicher Interviewpartner	–
3	berufliche Tätigkeit (Arbeitgeber, Funktion, Aufgaben, Berufserfahrung)	–
4	Berufliche Kontaktdaten (E-Mail, Telefon, Anschrift)	–
5	Tondateien der Interviews	–

Hinweis: Erfolgt eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten, so ist eine Datenschutz-Folgenabschätzung (siehe Ziffer 13) durchzuführen.

6 Kategorien betroffener Personen[1]

Lfd. Nr. aus 5.	Betroffene
1–5	Projektpartner und freiwillige Teilnehmende
1–5	Experten aus den Forschungsbereichen des Projekts

7 Rechtsgrundlage der Verarbeitungstätigkeit[2]

Lfd. Nr. aus 5.	**Bezeichnung der Vorschrift(en) oder Hinweis auf Einwilligung** (Einwilligungstext bitte als Anhang beifügen)	Erläuterungen
1,5	Einwilligung	
2,3,4	§ 35 LDSG BW, ab 25.5.2018 EU DSGVO: Art. 6 Abs 1 lit. e iVm Art. 6 Abs. 3 iVm § 4 LDSG BW 2018	2, 3, 4 werden für die Kontaktaufnahme benötigt; ist der/die Betroffene zu einem Interview bereit, werden zusätzlich die Daten 5 verarbeitet.

8 Empfänger personenbezogener Daten[1]

8.1 Interne Empfänger innerhalb der Organisation des Verantwortlichen

Lfd. Nr. aus 5.	Interne Stelle	Zweck
1	Projektmitarbeitende, Hilfskräfte	Transkription
5	Projektmitarbeitende, Hilfskräfte des IZEW	Transkription, Auswertung
2–4	Projektmitarbeitende	Kontaktaufnahme und Auswahl

8.2 Externe Empfänger

In der Spalte ADV ist ein „x“ zu setzen, wenn der Empfänger im Rahmen einer Auftragsverarbeitung tätig wird. Dann ist beim Zweck der Tätigkeitsumfang zu beschreiben.

Lfd. Nr. aus 5.	Empfänger, i.d.R. mit ladungsfähiger Anschrift	Zweck bzw. Tätigkeit	ADV
1–5	keine		

Sofern Empfänger ihren Sitz in einem Drittland haben oder es sich um eine internationale Organisation handelt:

Empfänger aus 8.2. mit Bezeichnung des Drittlandes	Die Weitergabe wird gestützt auf
	☐ einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m 47 DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch ein Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch folgende sonstige Maßnahmen (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO): ☐ folgenden Ausnahmetatbestand des Art. 49 DS-GVO:

9 Zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind[2]

Lfd. Nr. aus 5.	Personen(gruppe)	Umfang
1	Projektmitarbeitende, Hilfskräfte	lesend
5	Projektmitarbeitende, Hilfskräfte	lesend
2–4	Projektmitarbeitende	lesend und schreibend

10 Fristen für die Löschung[1]

Lfd. Nr. aus 5.	Frist
1	manuelle Löschung nach Abschluss der Transkription, nicht länger als Projektende (31. Oktober 2020)
5	manuelle Löschung bei Projektende (31. Oktober 2020). Im Falle eines nachträglichen Entzugs der Einwilligung unverzüglich.
2–4	Bei Nichtantwort auf Anfragen: 3 Monate nach Anfrage. Bei Nichtteilnahme an Interviews: 3 Monate nach Absage. Bei erfolgreicher Teilnahme bei Projektende (31. Oktober 2020)

11 Allgemeine Beschreibung der eingesetzten Hardware, Software und der Vernetzung[2]

11.1 Eingesetzte Software auf Klienten und Servern außer dem Betriebssystem

Lfd. Nr.	Art der Software	Bezeichnung	Version	Einsatz
1	Textverarbeitung	Microsoft Word	2016	☒ Klient ☐ Server
2	Wiedergabesoftware	VLC Player	3.0.1	☒ Klient ☐ Server
3	Transkriptionssoftware	f4	6.2.5	☒ Klient ☐ Server
4	Verschlüsselungssoftware	Veracrypt	1.21	☒ Klient ☐ Server
5	Qualitative Datenauswertung	NVIVO	11.4	☒ Klient ☐ Server
6	Qualitative Datenauswertung	ATLAS.ti	6	☒ Klient ☐ Server

11.2 Beteiligte Klienten (Arbeitsplatzrechner, mobile Rechner, Terminal, Videokamera usw.)

☐ Es handelt sich um eine Webanwendung, bei der die Klienten nicht näher bestimmbar sind.

Anzahl	Typ	Betriebssystem, Version	Software, lfd. Nr. aus 11.1	Netzwerk & Hardware	Daten, lfd, Nr. aus 5.
2	Laptop	Windows 10 Enterprise 1709	1,2,4–6	☒ IPv4 ☐ IPv6 ☒ SSD-Festplatte ☐ Ext. Medium	1–5
2	Workstation	Windows 7 Enterprise SP1	1,2,4–6	☒ IPv4 ☐ IPv6 ☐ SSD-Festplatte ☐ Ext. Medium	1–5
2	Workstation	Windows 10 Enterprise 1709	3,4	☒ IPv4 ☐ IPv6 ☒ SSD-Festplatte ☐ Ext. Medium	1,5

11.3 Beteiligte Server

Lfd. Nr.	Funktion	Betriebssystem, Version, Virtualisierung	Software, lfd. Nr. aus 11.1	Hardware	Standort	Daten, lfd. Nr. aus 5.
1	Arbeitsgruppenlaufwerk	Data On Tap 9.x ☒ virtualisiert		☒ SSD-Festplatte	Ort/Firma: ZDV ☐ extern ☒ intern Wächterstraße 76; Auf der Morgenstelle 24	1,5

11.4 Datensicherung

Lfd. Nr.	Medium	Server, lfd. Nr. aus 11.3	Software, lfd. Nr. aus 11.1	Aufbewahrungsort	Daten, lfd. Nr. aus 5.
–					

11.5 Darstellung der Netzstruktur

☒ Ist als folgende Anlage beigefügt: Netzdiagramm-NetApp-VV.pdf

11.6 Verwendete Protokolle, Dienste und Verschlüsselung

Übertragungsabschnitt	Software, lfd. Nr. aus 11.1	Protokoll, Port	Verschlüsselung
Datentransfer zwischen Klient und Arbeitsgruppenlaufwerk	4	SMB 3.1	Nicht eingesetzt

12 Technische und organisatorische Maßnahmen[1]

☐ Es wird auf folgendes Dokument verwiesen:

☒ Es sind (ggf. zusätzlich) folgende Maßnahmen getroffen:

12.1 Pseudonymisierung

Es werden bei 1 keine personenbezogenen oder identifizierenden Daten in die Transkription übernommen, sodass nach dieser eine Zuordnung der Aussagen zu Personen nicht mehr möglich ist. Bei 5 geschieht dies auf Wunsch des Interviewpartners ebenfalls.

12.2 Verschlüsselung

Alle Audiodateien werden nur in AES-256 verschlüsselten VeraCrypt-Containern gespeichert.

12.3 Gewährleistung der Vertraulichkeit

Auf das Arbeitsgruppenlaufwerk haben nur Mitarbeiter_innen des Projekts Zugriff, dies wird über die Windows-Rechteverwaltung umgesetzt. Für die Zugangskontrolle zu Serverräumen wird auf das ZDV verwiesen. Das Verschlüsselungspasswort besteht aus mindestens 12 Zeichen und ist nicht im Klartext digital gespeichert. Auf SSDs werden die Daten nur in VeraCrypt-Containern vorgehalten, bzw. werden die Daten 2–4 durch Überschreiben gelöscht.

12.4 Gewährleistung der Integrität

Verweis auf das ZDV der Universität Tübingen.

12.5 Gewährleistung der Verfügbarkeit

Regelmäßige, 18 Wochen zurückreichende, Snapshots und nächtliche Spiegelung der Daten durch das ZDV der Universität Tübingen.

12.6 Gewährleistung der Belastbarkeit der Systeme

Verweis auf das ZDV der Universität Tübingen.

12.7 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Verweis auf das ZDV der Universität Tübingen.

12.8 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Verweis auf das ZDV der Universität Tübingen.

12.9 Weitere Maßnahmen:

☐ Sensibilisierung und/oder Schulung der an Verarbeitungsvorgängen Beteiligten
☐ Beteiligung des/der zuständigen Datenschutzbeauftragten
☐ Hinweis/Verpflichtung der an Verarbeitungsvorgängen Beteiligten auf das Datengeheimnis
☐ Folgende Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind:
☐ Im Falle einer Übermittlung oder Zweckänderung:
Folgende spezifischen Verfahrensregelungen werden getroffen, um die Einhaltung des LDSG und der DS-GVO sicherzustellen:

☐ Sonstiges:

12.10 Weitere Dokumente:

☐ Interne Verhaltensregeln
☐ Risikoanalyse
☐ Allgemeine Datensicherheitsbeschreibung
☐ Umfassendes Datensicherheitskonzept
☐ Wiederanlaufkonzept
☐ Zertifikat:
Zertifizierungsstelle:
☐ Sonstiges:

13 Datenschutz-Folgenabschätzung[2]

☐ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist notwendig (insbesondere immer notwendig, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt).

☒ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist nicht notwendig.

Netzdiagramm NetApp: