Grant Agreement No.: 823783
Call: H2020-FETPROACT-2018-2020
Topic: H2020-FETPROACT-2018-01
Type of action: RIA

D9.3 A REVISED GUIDELINE CONCERNING PRIVACY-STANDARDS FOR WENET

Revision: v.1.0

Work package	WP 9
Task	Task 9.3
Due date	31/12/2020
Submission date	17/12/2020
Deliverable lead	EKUT
Version	1.0
Authors	Karoline Reinhardt (EKUT) Jessica Heesen (EKUT) Andreas Baur (EKUT) Amalia de Götzen (AAU) Christos Rodosthenous (OUC) Maria Chiara Campodonico (MARTEL) Daniele Miorandi (UH)
Reviewers	Kobi Gal (BGU)

Abstract	This deliverable contains the revised and amended guideline concerning privacy-standards for WeNet with descriptions of privacy norms for each component of the WeNet-project that is privacy-relevant.
Keywords	Privacy, GDPR, privacy-by-design and by-default

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	23/11/2020	1st draft version	Karoline Reinhardt (EKUT)
V0.2	27/11/2020	Sections added	Jessica Heesen (EKUT) Andreas Baur (EKUT)
V0.3	30/11/2020	Content added	Karoline Reinhardt (EKUT)
V0.4	02/12/2020	References and list of figures added	Karoline Reinhardt (EKUT)
V0.5	04/12/2020	Polishing of document, submitted for internal quality assessment	Karoline Reinhardt (EKUT)
V0.6	11/12/2020	Content added	Amalia de Goetzen (AAU) Christos Rodosthenous (OUC) Maria-Chiara (MARTEL) Daniele Miorandi (UHopper)
V0.7	14/12/2020	Comments from internal quality assessment incorporated	Karoline Reinhardt (EKUT)
V0.8	15/12/2020	Content added	Jessica Heesen (EKUT)
V0.9	15/12/2020	Structure adjusted	Karoline Reinhardt (EKUT)
V1.0	16/12/2020	Polishing of Document, submitted	Karoline Reinhardt (EKUT)

DISCLAIMER

COPYRIGHT NOTICE

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:		**R**
Dissemination Level		
PU	Public, fully open, e.g. web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to WeNet project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

Co-funded by the Horizon 2020
Framework Programme of the European Union

EXECUTIVE SUMMARY

WeNet acknowledges privacy as a fundamental principle and aims at implementing privacy-standards throughout its entire research phase as well as in the architecture and design of all the technological artefacts developed in the WeNet project.

In this deliverable we present the revised and amended guideline concerning privacy standards for WeNet. WeNet follows a threefold approach to privacy that refers to the implementation of legal requirements, the technical implementation of a privacy-by-design and privacy-by-default and the data protection forum for the discussion of open and upcoming questions. This threefold approach to privacy was developed in the preliminary guideline concerning privacy standards for WeNet. The deliverable at hand builds upon this approach to privacy and further elaborates it taking up developments in the research on privacy as well as in the technical infrastructure of WeNet.

The guideline starts with outlining general ethical principles concerning privacy standards for WeNet, such as transparency, fairness, purpose limitation, data minimisation, accuracy, storage limitation, data security, accountability, privacy-by-design and by-default, protection of minors, monitoring and iterated evaluation and enhancement of privacy literacy. Then, these principles are applied to the central components of WeNet's research process and its technical elements. The guideline proceeds on the implicit assumption that all legal rights and obligations that apply to the processes and activities of WeNet are mandatory and must be duly observed.

Co-funded by the Horizon 2020
Framework Programme of the European Union

TABLE OF CONTENTS

Co-funded by the Horizon 2020 Framework Programme of the European Union

Co-funded by the Horizon 2020
Framework Programme of the European Union

LIST OF FIGURES

Co-funded by the Horizon 2020
Framework Programme of the European Union

ABBREVIATIONS

AAU	Aalborg Universitet
BGU	Ben Gurion University of the Negev
D	Deliverable
DPF	Data Protection Forum
EKUT	Eberhard Karls Universität Tübingen
EU	European Union
GDPR	General Data Protection Regulation
JLU	Jilin University
LSE	London School of Economics and Political Science
M	Project month
NUM	National University of Mongolia
OUC	Open University Cyprus
RI	Research Infrastructure
UC	Universidad Católica Nuestra Señora de la Asunción
UH	UHopper SRL
UNITN	Università degli studi di Trento
WP	Work package

Co-funded by the Horizon 2020
Framework Programme of the European Union

1. INTRODUCTION

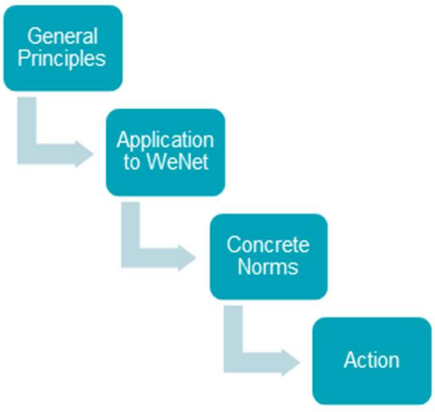
WeNet will provide a diversity-aware, machine-mediated paradigm for social interaction that transcends geographical and cultural backgrounds. Diversity-awareness presupposes the collection of diversity-related data. Diversity-related data are, however, sensitive and, thus, their collection increases the vulnerability of data subjects to various kinds of misuse scenarios – online and offline. Securing data privacy standards is therefore of utmost importance.

WeNet acknowledges privacy as a fundamental principle and aims at implementing privacy-standards throughout its entire research phase as well as in the architecture and design of all the technological artefacts developed in the WeNet project.

WeNet has therefore formulated “A Preliminary Guideline concerning Privacy-Standards” [1]. During the past year the technology and infrastructure developed in WeNet as well as the research about privacy and privacy standards from ethical, legal and social sciences perspectives has evolved. These more recent developments, debates and discourses bring about new questions but also promising possibilities to deal with threats to privacy in WeNet. The aim of this deliverable is to revise and amend the preliminary privacy-guideline taking the technological advances in WeNet into account while also implementing the findings and research results with regard to privacy that where made since the publication of the preliminary guideline in 2019.

WeNet follows a threefold approach with regard to privacy. This threefold approach is based on a) the implementation of the GDPR, b) a privacy-by-design and by-default approach, and c) actions and activities in the WeNet Data Protection Forum (DPF). We will recapitulate this threefold approach and its main principles in section 2. During the research process it became more and more apparent that notions like contextual privacy, responsibility for privacy and privacy literacy need to be implemented in WeNet’s privacy-standards. We discuss these notions in sections 3-5. Section 6 contains the revised and amended guideline concerning privacy-standards for WeNet.

FIGURE 1: FROM PRINCIPLE TO PRACTICE



In this guideline, we first formulate general principles of privacy WeNet shall adhere to in all its actions and technological developments. These abstract principles are translated in concrete norms with regard to all central elements of WeNet that are relevant to privacy. For each element, we provide a short description of how it works with a particular focus on the aspects that are relevant regarding privacy. After that, we will specify privacy enhancing norms in line with the general principles formulated. Section 7 summarizes the work done and outlines the next steps to be taken by WeNet with regard to privacy. The norms

Co-funded by the Horizon 2020 Framework Programme of the European Union

formulated are in a next step to be translated into concrete actions [see figure 1]. Special attention will be paid to future challenges and to possible abuse scenarios and risks for WeNet users.

We would like to emphasize that all natural and legal persons have a duty to comply with law – applicable today, or in the future. The guideline, thus, proceeds on implicit the assumption that all legal rights and obligations that apply to the processes and activities of WeNet are mandatory and must be duly observed. This document thus provides *ethical* guidance with regard to privacy and on how to implement abstract principles into concrete measures.

Co-funded by the Horizon 2020
Framework Programme of the European Union

2. WENET'S APPROACH TO PRIVACY

"In today's digital environment adherence to law is not enough; we have to consider the ethical dimension of data processing" [2]

WeNet aims at providing a diversity-aware machine mediated paradigm for social relations and interactions. At the basis of WeNet is the WeNet platform, which is the basis for a number of studies across the world with diverse student populations. A platform that is diversity-aware is storing, processing and managing sensitive personal data. Therefore, data and privacy protection play a crucial role within the WeNet project.

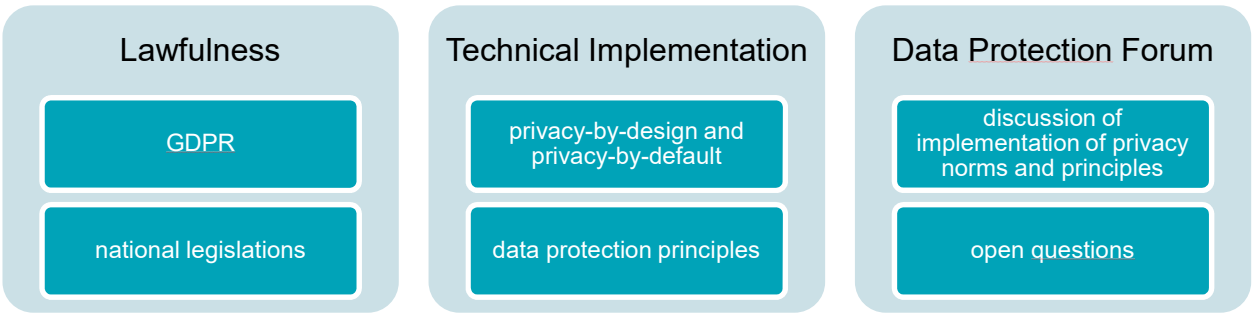
Privacy is necessary for people to freely unfold and develop their personality and identity. It consists in the definition of aspects of our lives as protected from external interference. The protection of privacy includes the protection of private spaces, anonymity as privacy in public spaces, the right to informational self-determination as well as integrity of personal identity. Anonymity means the freedom not to be identified and systematically observed. Informational self-determination is the right to decide whether personal data are to be disclosed and used. The integrity of personal identity includes the right to informational self-determination and self-representation as well as protection against misrepresentation. This includes insults and defamation as well as the creation of (falsely) predictive personality profiles [3].

Privacy has different dimensions, such as informational, physical or spatial privacy. The requirements arising for the protection of privacy and the right to informational self-determination depend on the respective contextual conditions. With regard to information technologies privacy requires, for instance, transparency of data protection regulations, minimization of data collection and processing, in particular personal data and a privacy-by-design approach [3].

WeNet acknowledges privacy as a fundamental principle and aims at implementing privacy-standards throughout its entire research phase as well as in the architecture and design of all the technological artefacts developed in the WeNet project.

The WeNet approach to privacy consists of three elements [see figure 2]: legal standards such as the GDPR, a privacy-by-design and by-default with regard to technological artefacts (such as the WeNet-Platform and WeNet-Apps) and a Data Protection Forum (DPF) for all unforeseen upcoming privacy issues.

FIGURE 2: WENET'S THREEFOLD APPROACH TO PRIVACY



Co-funded by the Horizon 2020 Framework Programme of the European Union

2.1 LAWFULNESS

WeNet operates within a world that is bound to numerous privacy laws and regulations. It need not be underlined that WeNet is committed to the adherence to current law and will comply with all applicable laws and regulations. It is important to note, however, that: "The law provides both positive and negative obligations, which means that it should not only be interpreted with reference to what *cannot* be done, but also with reference to what *should* be done and what *may* be done" [4].

The GDPR is the major legal sources for privacy standards and data protection in WeNet. Article 5 GDPR states principles related to the processing of personal data that are highly relevant for WeNet: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. Lawfulness for the purposes of the WeNet privacy guideline will be taken as a standard basis of all actions: The guideline proceeds on the implicit assumption that all legal standards, rights and obligations that apply to the processes and activities in WeNet are mandatory and must be duly observed.

The norms of the GDPR are, of course, in many places highly abstract and there is, compared to other legal standards that are much older, less experience with how to implement the principles of the GDPR into practice. WeNet, thus, is also a case study in how to apply these abstract legal norms into concrete practices and technological solutions. Wherever the law does not yet prescribe details for certain technical innovations, action shall be taken in the spirit of existing legislation.

Since WeNet, however, works in an evolving and highly dynamic field of research, it should also take into account what should be done from an ethical perspective with regard to privacy protection beyond its commitment to compliance with existing legal standards. This includes technological solutions as well as the dialogue with data subjects and users: The implementation of privacy protection cannot be standardised by legal regulations alone (such as regulations on data minimisation or purpose limitation), but must be realised through a careful and trustworthy design of the technology itself. Furthermore, WeNet has to strive for empowering digital media users and in particular the users of WeNet through technological set up and educational material, tutorials and courses.

2.2 PRIVACY-BY-DESIGN AND BY-DEFAULT

As mentioned above, the implementation of privacy protection cannot be standardised by legal regulations alone, but must be realised through the design of the technology itself and the cooperation between experts for ethics, computer science and sociology. Therefore, WeNet conducts integrated research and follows a privacy-by-design and a privacy-by-default approach.

Privacy-by-design approaches secure certain data protection standards with technical means.

Privacy-by-default is based on data protection-friendly default settings.

The foundational principles of privacy-by-design and by-default are [7]:

- *"Privacy as the Default Setting":* Privacy shall be the default setting.
- *"Proactive not Reactive; Preventative not Remedial"*: Anticipate and prevent privacy violations and do not wait for privacy risks to materialise. Privacy-by-design comes before-the-fact, not after.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- *"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.

- *"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.

- *"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.

- *"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.

- *"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.

We can derive several design strategies from a privacy-by-design approach [8]:

- *"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'.

- *"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.

- *"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.

- *"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 requirement, thus, is anonymisation.

- *"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.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- *"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.

- *"Enforce"*: There should be a privacy policy in place that is compatible with legal requirements and this privacy policy should be enforced.

- *"Demonstrate"*: There shall 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.

WeNet shall follow these design-strategies.

2.3 DATA PROTECTION FORUM

We follow an integrated research approach in WeNet. The starting point of an integrated research approach is the observation that the development of new technologies needs to consider ethical, social, legal and economic aspects. Therefore, integrated research is interdisciplinary and process oriented. It integrates these various perspectives from the get go by raising awareness in particular for ethical questions (see also [4]). The goal is to make technical innovations more ethically aware and socially sensitive. Ethics, thus, becomes a task for all project partners.

As mentioned above, the implementation of privacy protection must be realised through the design of the technology itself. Therefore, privacy-standards need to be implemented from the very beginning of the development process and ethical considerations need to be taken into account. To facilitate the discussion on privacy standards and data protection in WeNet, we have launched the Data Protection Forum (DPF) as one important instrument of integrated research in WeNet.

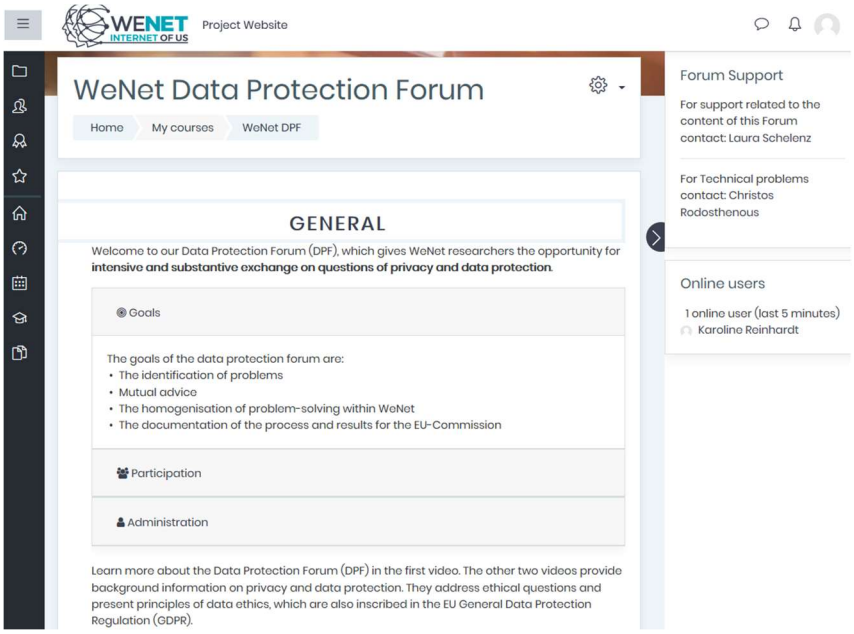
The DPF gives WeNet-researchers a platform for intensive and substantive exchange on questions of privacy and data protection. It helps to identify problems early on, facilitates mutual advice-giving, and homogenizes a problem-solving with regard to data protection and privacy issues. It will also help to develop new and innovative concepts and methods for interdisciplinary integrated research. The Forum consists of an online tool and a series of workshop formats.

The online tool invites WeNet researchers to start a conversation on privacy and data protection. It is a platform where researchers can collect questions and problems that arise during our work in WeNet and discuss possible solutions. The online forum has three branches: questions concerning data collection, questions concerning data processing and questions concerning data storage. Further topics can be added as needed. It would be desirable for this instrument to be even more widely adopted and used. We are currently reflecting on further activation methods to involve the Consortium even more in the discussions and to raise the awareness of the various researchers in WeNet for the exchange on privacy issues.

Co-funded by the Horizon 2020
Framework Programme of the European Union

The online DPF is part of the WeNet eLearning Platform[1], which hosts WeNet's online courses that are available to students and the general public [see figure 3]. It is based on Moodle, an open source learning content management system, and offers distance learning courses, collaboration tools and self-evaluation activities along with educational content that is designed to guide and introduce students to the WeNet's project topics. Interested users can create an account and join the available courses. The DPF is, however, so far only open to WeNet researchers to provide the necessary confidentiality of the discussion, but WeNet will decide in due time, whether and in what way this online tool could also be of use to students participating in the pilots to give them a voice with regard to privacy issues in WeNet.

FIGURE 3: WENET DATA PROTECTION FORUM ON THE WENET ELEARNING PLATFORM



Unfortunately, due to the corona pandemic, it was not possible to implement the offline part of the Data Protection this year to the extent planned. However, after a period of adaptation to the new working methods, we were able to hold some digital meetings on privacy issues with small groups from the consortium.

Questions that we have addressed so far in the DPF include, but are not limited to ethical questions with regard to data collection, data processing, data storage, trustworthiness of a future WeNet-application, agency and data control, transparency with regard to incentives design and privacy in profiling.

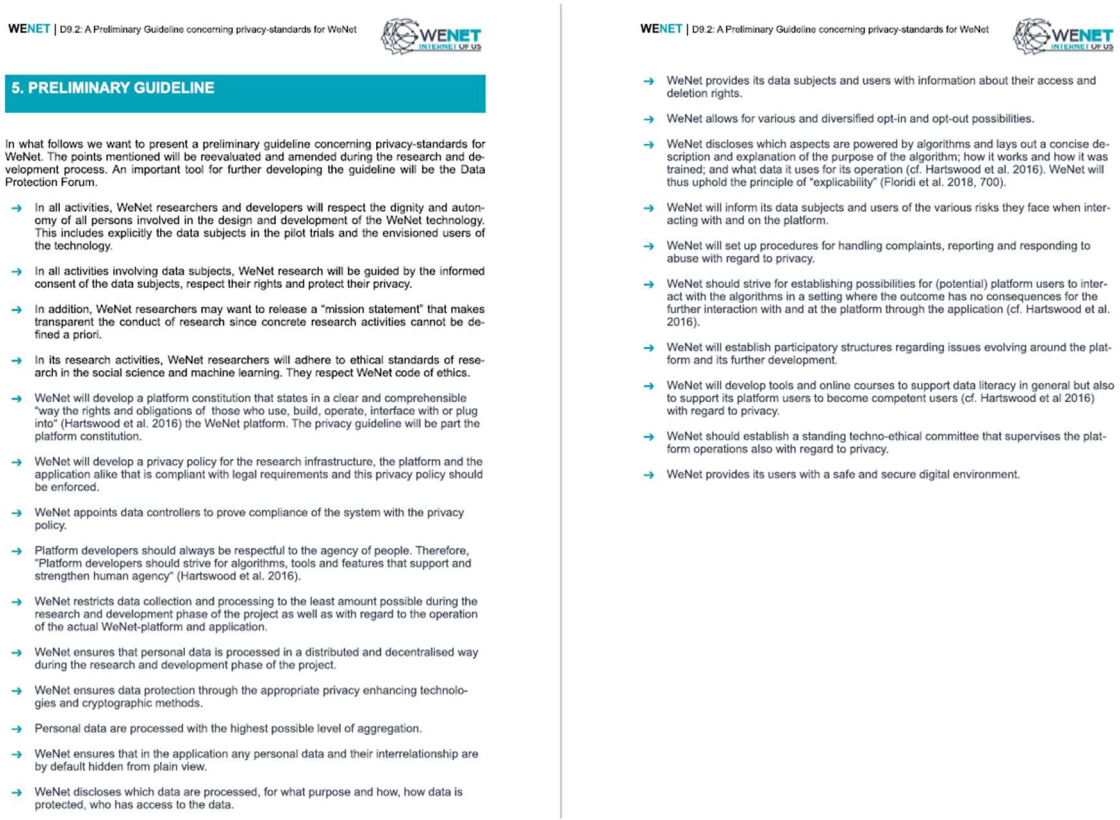
2.4 PRELIMINARY GUIDELINE TO PRIVACY

Taking up considerations on legal and ethical standards, WeNet has formulated a preliminary guideline concerning privacy-standards in WeNet in 2019 [1] [see figure 4].

[1] The eLearning platform can be found at https://elearning.internetofus.eu.

Co-funded by the Horizon 2020 Framework Programme of the European Union

FIGURE 4: PRELIMINARY GUIDELINE CONCERNING PRIVACY-STANDARDS IN WENET



WENET | D9.2: A Preliminary Guideline concerning privacy-standards for WeNet

5. PRELIMINARY GUIDELINE

In what follows we want to present a preliminary guideline concerning privacy-standards for WeNet. The points mentioned will be reevaluated and amended during the research and development process. An important tool for further developing the guideline will be the Data Protection Forum.

- In all activities, WeNet researchers and developers will respect the dignity and autonomy of all persons involved in the design and development of the WeNet technology. This includes explicitly the data subjects in the pilot trials and the envisioned users of the technology.
- In all activities involving data subjects, WeNet research will be guided by the informed consent of the data subjects, respect their rights and protect their privacy.
- In addition, WeNet researchers may want to release a "mission statement" that makes transparent the conduct of research since concrete research activities cannot be defined a priori.
- In its research activities, WeNet researchers will adhere to ethical standards of research in the social science and machine learning. They respect WeNet code of ethics.
- WeNet will develop a platform constitution that states in a clear and comprehensible "way the rights and obligations of those who use, build, operate, interface with or plug into" (Hartswood et al. 2016) the WeNet platform. The privacy guideline will be part the platform constitution.
- WeNet will develop a privacy policy for the research infrastructure, the platform and the application alike that is compliant with legal requirements and this privacy policy should be enforced.
- WeNet appoints data controllers to prove compliance of the system with the privacy policy.
- Platform developers should always be respectful to the agency of people. Therefore, "Platform developers should strive for algorithms, tools and features that support and strengthen human agency" (Hartswood et al. 2016).
- WeNet restricts data collection and processing to the least amount possible during the research and development phase of the project as well as with regard to the operation of the actual WeNet-platform and application.
- WeNet ensures that personal data is processed in a distributed and decentralised way during the research and development phase of the project.
- WeNet ensures data protection through the appropriate privacy enhancing technologies and cryptographic methods.
- Personal data are processed with the highest possible level of aggregation.
- WeNet ensures that in the application any personal data and their interrelationship are by default hidden from plain view.
- WeNet discloses which data are processed, for what purpose and how, how data is protected, who has access to the data.

WENET | D9.2: A Preliminary Guideline concerning privacy-standards for WeNet

- WeNet provides its data subjects and users with information about their access and deletion rights.
- WeNet allows for various and diversified opt-in and opt-out possibilities.
- WeNet discloses which aspects are powered by algorithms and lays out a concise description and explanation of the purpose of the algorithm; how it works and how it was trained; and what data it uses for its operation (cf. Hartswood et al. 2016). WeNet will thus uphold the principle of "explicability" (Floridi et al. 2018, 700).
- WeNet will inform its data subjects and users of the various risks they face when interacting with and on the platform.
- WeNet will set up procedures for handling complaints, reporting and responding to abuse with regard to privacy.
- WeNet should strive for establishing possibilities for (potential) platform users to interact with the algorithms in a setting where the outcome has no consequences for the further interaction with and at the platform through the application (cf. Hartswood et al. 2016).
- WeNet will establish participatory structures regarding issues evolving around the platform and its further development.
- WeNet will develop tools and online courses to support data literacy in general but also to support its platform users to become competent users (cf. Hartswood et al 2016) with regard to privacy.
- WeNet should establish a standing techno-ethical committee that supervises the platform operations also with regard to privacy.
- WeNet provides its users with a safe and secure digital environment.

Since then the technology and infrastructure developed in WeNet have evolved as well as the research about privacy and privacy standards from ethical, legal and social sciences perspectives. These more recent developments, debates and discourses bring about new questions regarding privacy, but also interesting possibilities to deal with threats to privacy in WeNet. However, the revision of the guideline also reflects the conviction that as in all technology development processes even with careful consideration it is not possible to predict all effects and side effects of a given technology. It is, thus, recommendable to define and implement iterated evaluation procedures. The revision and amendment of the privacy-guideline is such an iterated evaluation procedure.

Co-funded by the Horizon 2020 Framework Programme of the European Union

3. DIVERSITY AND PRIVACY

WeNet Project is committed to both diversity and privacy. During the research process in WeNet the tension between these two commitments became more and more apparent. To learn and discover diversity patterns as well as to ensure that diversity is instantiated in WeNet, the collection, evaluation and storage of diversity-related data is necessary. Diversity-related data consist of personal and sensitive data. Their collection, usage and storage come with a number of (potential) risks to privacy. These include but are not limited to identity theft, malicious attacks on the data management system and a resulting ungovernable diffusion of data. However, to create meaningful profiles and matching mechanisms, as well to learn diversity from data and for the design of diversity-sensitive interaction protocols data collection is necessary.

Furthermore, since diversity dimensions are fluid and context-dependent, the possibility of independent control for users of how they are represented on a platform is particularly important. It is, for instance, conceivable that identity management here entails also that seemingly private information, such as a form of disability, can be released by the person concerned. What is needed is a contextual understanding of privacy that allows for different spheres of privacy that are guided by different norms for the interaction and information flows that take place in them [17].

Furthermore, due to the rapidity of innovation in the field of data driven technologies and the rapid progress in the performance of information technology systems, there is a need for continuous social discussion and adaptation of privacy concepts and principles in order to secure their value for democracy under changed conditions. It is, therefore, important at this point to see privacy not as a static but as a dynamic concept, which is undergoing permanent renegotiation in relation to digital technologies of all kinds. This requires users to be able to assess their actions online and to weigh the intended consequences with unintended side effects.

Finally, privacy nevertheless requires – conceptually as well as structurally – certain preconditions that have to be met to allow for privacy in general and various spheres of privacy in particular. In the guideline, we outline such preconditions.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4. RESPONSIBILITY FOR PRIVACY

The WeNet project has to guarantee privacy protection at all stages of the research process and the development process of the technical solutions. In accordance with GDPR requirements, WeNet clearly and transparently states who is accountable for which aspects of the data collection process and with regard to the storage and further processing of data with respect to data protection and privacy.

Being legally accountable for actions and being responsible are overlapping but not synonymous concepts. What is needed, is a multidimensional understanding of responsibility that entails (but is not limited to) notions of positive, that is proactive, responsibility, consumer/user responsibility, professional responsibility and framework responsibility.

For WeNet it is, thus, important that all parties involved in research and development processes are privacy aware and act accordingly. To enhance privacy awareness fostering constructive exchange and discussion of privacy related matters between the various disciplines involved WeNet is imperative. The DPF as well as other integrated research methods provides an adequate exchange framework for these questions in WeNet.

Co-funded by the Horizon 2020
Framework Programme of the European Union

5. PRIVACY LITERACY

As mentioned above, in view of the ever-increasing risks for the protection of privacy with regard to information technology systems, demands for privacy literacy are becoming increasingly frequent. Privacy literacy means that users of digital media should possess the knowledge and skills necessary to protect their privacy when using these media. Through means of education, users of digital media are to be empowered to use digital media, digital platforms and services in such a way that their own privacy is protected. The overall goal is to enable users of digital media to control personal information as comprehensively as possible and to counteract increasingly urgent privacy risks [6].

Accordingly, privacy literacy encompasses a whole range of competencies. These include, but are not limited to

- Ability to reflect
  - Why private data should be classified as worthy of protection (ethical competence) [5]
  - On power aspects of digitization and digitalization (systemic analysis and political knowledge) [5]
  - On the consequences that could result from the publication of private data (risk competence) [5]
- Knowledge
  - About data protection laws and data protection institutions
  - About providers and practices of online platforms and services, in particular knowledge of who collects, processes and passes on private data for what purpose (structural competence) [5]
  - About strategies regarding the individual regulation of one's own privacy
  - About technical aspects of the operation and use of data protection tools, such as privacy settings, self-protection tools, or privacy enhancing technologies (competence to act) [5]
  - On how media communicate and construct privacy (mediality competence) [5]
- Competence and skills to act accordingly

With regard to the technical aspect, privacy literacy thus touches on aspects of computer literacy.

The call for “privacy literacy” is often regarded as an answer to the problem of the “privacy paradox” [6]. The “privacy paradox” states that there is a discrepancy between the statements about the importance of protecting one's own privacy and the concrete behaviour of media use, in which little attention is paid to the protection of privacy. Knowledge about privacy and the according competencies is an important aspect of mitigating the discrepancy between conviction and action with regard to privacy protection.

WeNet is committed to privacy literacy in a number of ways and supports various activities in this field, for instance:

- Scientific publications on privacy
- Production of educational courses and training material as part of the Open Online Course and development, participation and organization of educational courses concerning privacy literacy in other settings.
- Talks and presentations on data and privacy literacy for students and researchers by members of the WeNet consortium

Co-funded by the Horizon 2020 Framework Programme of the European Union

- "Science to Public" activities on privacy and privacy protection by members of the WeNet consortium.

It is worth noting, however, that privacy literacy though an important aspect of privacy protection is not the answer to all issues and problems in this area. There are, however, a number of problems regarding privacy literacy that we need to bear in mind.

First, people's abilities to become privacy literate are very different. For instance, while people with a low socio-economic status are more likely to be at risk of having their privacy violated by economic or governmental institutions, they are less often in a position to become "privacy literate" through education for a lack of material and immaterial resources [6]. Conversely, persons who are most likely to acquire privacy literacy through education also tend to experience fewer institutional violations of privacy due to their rather high socio-economic status in the first place [6].

Secondly, there is the problem that research on privacy literacy tends to assume that users of digital media are rational actors who carry out cost-benefit calculations in the disclosure of information or weigh risks against benefits [6]. However, due to affective or even irrational aspects of media usage as well as routine-based behaviour with digital tools, persons often do not call upon even existing knowledge about methods and techniques of privacy protection.

Thirdly, privacy literacy is mainly concerned with front-end features, for instance with privacy or data protection settings that can be made on the user interfaces of platforms and services. Privacy violations, however, often take place "behind" the user interfaces, where methods of social profiling, machine learning or data mining are used.

Fourthly, the discourse on privacy literacy puts the burden of privacy protection on the shoulders of the individual users of digital media [6]. Privacy is, however, not a private matter. Individuals can never effectively ensure the protection of their own privacy, among other things because of their lack of insight and regulatory options vis-à-vis providers and platform operators. Institutionalized forms of regulation are nevertheless needed as well. Political processes, however, take time. For the time being, we need a heightened sense of responsibility for privacy protection by researchers, developers and designers.

Thus, the call for media, data and privacy literacy can quickly lead, however, to excessive demands on users, but also on companies or the public sector, if democratic use of technology is not framed and shaped by appropriate infrastructures. In light of these difficulties, privacy literacy should not be mistaken for a general "solution".

WeNet therefore takes its responsibility to contribute to the development of privacy literacy seriously. This also means that WeNet does not leave it up to the users alone to educate themselves in this area, but already offers corresponding materials. At the same time, WeNet is aware that privacy literacy alone is not a solution to privacy issues and problems. Therefore, WeNet pursues a strong privacy-by-design approach as a guiding principle for the work in WeNet.

Co-funded by the Horizon 2020 Framework Programme of the European Union

6. REVISED AND AMENDED PRIVACY-GUIDELINE

In what follows we want to present the revised and amended guideline concerning privacy-standards for WeNet.

➔ The guideline proceeds on the implicit assumption that all legal standards, rights and obligations, that apply to the processes and activities in WeNet are mandatory and must be duly observed. If the law does not yet prescribe details for certain technical innovations, action shall be taken in the spirit of existing legislation.

➔ In all activities, WeNet researchers and developers will respect the dignity and autonomy of all persons involved in the design and development of the WeNet technology. This includes explicitly the data subjects in the pilot trials and the envisioned users of the technology.

➔ In its research activities, WeNet researchers will adhere to ethical standards of research in the social science and machine learning. They will, furthermore, respect WeNet's internal code of conduct [see internal deliverable 11.2, appendix B].

➔ WeNet is committed to provide its data subjects with a safe and secure digital environment.

➔ In all activities involving data subjects, WeNet research will be guided by the informed consent of the data subjects, respect their rights and protect their privacy.

➔ Platform developers should always be respectful to the agency of people. Therefore, "Platform developers should strive for algorithms, tools and features that support and strengthen human agency"[10].

6.1 GENERAL PRINCIPLES CONCERNING PRIVACY IN WENET

6.1.1 Transparency

Transparency is a central requirement of data protection: In order for people to give their sovereign and informed consent to the transfer of data, there must be transparency regarding the way in which data is collected, evaluated and used [3].

Data subjects have, both legally and ethically, a right to transparent information and a right to information on where and what personal data are collected from the data subject and where not. The information given to data subjects shall be in a clear and plain language.

The data subjects have, both legally and ethically, the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.

They also have the right to the following information:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations

Co-funded by the Horizon 2020 Framework Programme of the European Union

- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- the right to lodge a complaint with a supervisory authority
- information on, where the personal data are not collected from the data subject, any available information as to their source
- the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

A central prerequisite of transparency is interpretability and explainability.

6.1.2 Fairness

It must be ensured that data collected about individuals will not be used to unfairly discriminate against them. The values inscribFed in technologies developed in WeNet have to be constantly reflected with regard to their ethical aptness. This must be given particular attention wherever there is a risk of stereotypes finding their way into the technical infrastructure. Furthermore, researchers in WeNet shall pay particular attention to situations, which involve particularly vulnerable groups, or power asymmetries or information asymmetries [4].

6.1.3 Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Accordingly, the data subject has, both ethically and legally, the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. The controller is obliged to erase personal data without undue delay, if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

6.1.4 Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6.1.5 Accuracy

Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Accordingly, each data subject has both ethically and legally a right to rectification. Furthermore, each data subject has, again: both ethically and legally, the right to obtain from the controller restriction of processing, if the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

6.1.6 Storage Limitation

Personal data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes in subject to implementation of the appropriate technical and organisational measures required are taken in order to safeguard the rights and freedoms of the data subject.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Accordingly, the data subject has, both ethically and legally, the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

Furthermore, each data subject has, both ethically and legally, the right to obtain from the controller restriction of processing, if, though, the controller no longer needs the personal data for the purposes of the processing, but the data are required by the data subject for the establishment, exercise or defence of legal claims.

6.1.7 Data Security

In accordance with GDPR, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.1.8 Accountability

Whether and in what cases those developing the system are liable for possible damage must be clarified clearly and transparently. For even if developers and providers make an effort to carry out an ethically reflected technology development process, it cannot be ruled out that the technologies developed in WeNet may cause damage from time to time. In such cases, there must be accountability and the resulting damage must be compensated in the best possible way [13].

A first step in this direction is WeNet's appointment of data controller to ensure accountability. The data controller is responsible for the compliance with the GDPR principles and shall be able to demonstrate this compliance. However, what happens in cases of damage due to the developed architecture and research infrastructure (RI) needs still further specification – in particular regarding the time after the WeNet project has ended.

6.1.9 Privacy-by-Design and by-Default

WeNet shall follow a privacy-by-design and a privacy-by-default approach as described above (see 2.2).

6.1.10 Protection of Minors

Children and minors merit specific protection with regard to their personal data. They may be less aware of the risks, consequences and of their rights when personal data are processed. They are also particularly vulnerable to privacy threats and are often unaware how their digital footprint will affect them in the future. WeNet shall ensure that it complies with the respective national legislation on the protection of children and minors.

6.1.11 Monitoring and Iterated Evaluation

As mentioned above, as in all technology development processes, even with careful consideration, it is not possible to predict all effects and side effects of a given technology. Therefore, it is recommendable to define and implement monitoring and evaluation procedures that determine when and in what form the now unforeseeable side effects are examined, and the RI and technologies adjusted. These evaluation procedures have to be iterated over time.

6.1.12 Enhancing Privacy Literacy

Privacy literacy means that users of digital media should possess the knowledge and skills necessary to protect their privacy when using these media. The overall aim is to enable users of digital media to control personal information through careful design and understandable information as comprehensively as possible and to counteract increasingly urgent privacy

Co-funded by the Horizon 2020 Framework Programme of the European Union

risks. Through means of education, users of digital media are to be empowered to use digital media, digital platforms and services in such a way that their own privacy is protected.

6.2 RESEARCH INFRASTRUCTURE AND PRIVACY

The WeNet consortium develops a research infrastructure (RI) that will allow the exploitation of the project results. The WeNet RI is an e-infrastructure capable of managing the full lifecycle of data generated in the WeNet pilot experiments (collection, processing, storage, access). As such, the RI comprises a set of software enablers for data collection and analysis, together with online training material and protocols for running experiments and trials and enable scientists to access them in compliance with existing regulations and WeNet's ethical principles (including privacy) [10]. WeNet will define a set suitable business models for the RI. Besides that WeNet will ensure the availability of the Infrastructure after the end of the project, and, possibly, become an official European RI.

Transparency

- WeNet commits to transparency with regard to its RI.
- WeNet shall declare in plain and easily comprehensible language how and what data are managed and stored in the RI and who has access to these data.

Fairness

- The values inscribed in the set up of the RI shall be constantly reflected with regard to their ethical aptness.

Purpose Limitation

- Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Further processing for achieving scientific research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. However, WeNet has to ensure verification of the scientific purpose before allowing scientists outside the WeNet consortium to access data.

Accuracy

- WeNet shall ensure that personal data stored, processed and managed in the RI shall be accurate and, where necessary, kept up to date.
- WeNet shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- WeNet shall respect each data subject's right to rectification
- WeNet shall respect each data subjects right to obtain from the controller restriction of processing, if the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

Data Security

- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- WeNet shall implement appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of pro-cessing systems and services.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet shall implement appropriate technical and organisational measures to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Accountability

- The Data Management in WeNet shall lie with the Project Management. It shall be in charge of ensuring coherent management of research data collected in the project and processed by the partners.
- WeNet shall appoint data controllers to prove compliance of the system with the privacy policy.
- WeNet shall set up procedures for handling complaints, reporting and responding to abuse with regard to privacy and the RI particularly for the time after the WeNet project has ended.

Privacy-by-design

- WeNet shall follow a privacy-by-design Approach also with regard to the RI. Key elements regarding the RI are anonymization and aggregation of as well as decentralisation of data processing. Furthermore, appropriate data security measures.

Monitoring and Iterated Evaluation

- WeNet shall develop a privacy policy for the RI, the platform and the application alike that is compliant with legal requirements and this privacy policy shall be enforced.
- WeNet shall implement internal procedures and policies aimed at securing compliance with data protection laws to help to facilitate ethical data handling [4].
- WeNet shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- The set up of the RI shall be re-evaluated in reasonable intervals also from an ethical perspective and with particular care for privacy issues.

6.3 WENET PLATFORM AND PRIVACY

WeNet designs an online platform to support the pilots leveraging diversity while empowering interactions effectively. The WeNet platform consists of a set of modular, interoperable, open software components providing the required functionality to enable the fast development and deployment of diversity-aware applications. The WeNet platform will therefore support a plurality of applications (be them mobile, web or chat apps), which will leverage the functionality exposed by the platform. Applications by registered developers will interact through the platform through a set of purposeful APIs. A special case of diversity-aware applications is the WeNet app, which will be developed by the Consortium and used throughout the pilot sites. The platform is able to connect to third-party services and applications, including but not limited to, mobile phone sensors (through a mobile app), calendar applications, social media streams, open data portals etc. Data streams from said third-party services and applications are used – by means of advanced AI/ML methods and algorithms, to personalise the user experience and to properly account for diversity dimensions [10]. With regard to exploitation planning a set of business models will be defined and empirically validated with the relevant stakeholders. WeNet is nonetheless committed to openness and transparency; accordingly, an open source “community” edition of the WeNet platform software toolkit will be released and maintained.

Transparency

- WeNet commits to transparency with regard to its platform architecture and platform management.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet shall inform its data subjects and users of the various risks they face when interacting with and on the platform.
- WeNet shall declare how and what data are managed and stored and who has access to these data.
- WeNet shall provide its data subjects with information on the categories of personal data concerned, that is what kind of data is collected.
- WeNet shall provide its data subjects with information on the recipients or categories of recipient to whom the personal data have been or will be disclosed.
- WeNet shall provide its data subjects, where possible with information on the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- WeNet will inform data subjects that it may store personal data for longer periods for achieving scientific research purposes.
- WeNet shall provide its data subjects with information on the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- WeNet shall provide its data subjects with information on the right to lodge a complaint with a supervisory authority.
- WeNet shall provide its data subjects with information on, where personal data are not collected from the data subject.
- WeNet shall provide its data subjects with any available information as to the source of the personal data collected.
- WeNet shall provide its data subjects with information on the existence of automated decision-making, including profiling.
- WeNet shall provide its data subjects with meaningful information about the logic involved in the automated decision-making, as well as the significance and the envisaged consequences of such processing for the data subject.
- WeNet shall provide the possibility for the data subjects to access their personal data.
- WeNet shall develop a platform constitution that states in a clear and comprehensible "way the rights and obligations of those who use, build, operate, interface with or plug into" (Hartswood et al. 2016) the WeNet platform. The privacy policy shall be part the platform constitution.

Fairness

- The values inscribed in the set up of the platform architecture shall be constantly reflected with regard to their ethical aptness.
- WeNet shall ensure that data collected about individuals will not be used to unfairly discriminate against them.
- WeNet shall pay particular attention wherever there is a risk of stereotypes finding their way into the technical infrastructure. Furthermore, researchers in WeNet shall pay particular attention to situations, which involve particularly vulnerable groups, or power asymmetries or information asymmetries [4].

Purpose Limitation

- Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Further processing for achieving scientific research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data Minimisation

- WeNet restricts data collection and processing to the least amount possible.
- Personal data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Accuracy

- WeNet shall ensure that personal data stored, processed and managed on the platform shall be accurate and, where necessary, kept up to date.
- WeNet shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- WeNet shall respect each data subject's right to rectification.
- WeNet shall respect each data subject's right to obtain from the controller restriction of processing, if the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

Data Security

- WeNet shall ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- WeNet shall implement appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of pro-cessing systems and services.
- WeNet shall implement appropriate technical and organisational measures to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Accountability

- The Data Management in WeNet shall lie with the Project Management. It shall be in charge of ensuring coherent management of research data collected in the project and processed by the partners.
- WeNet shall appoint data controllers to prove compliance of the system with the privacy policy.
- WeNet shall set up procedures for handling complaints, reporting and responding to abuse with regard to privacy for the platform – particularly with regard to the time after the WeNet project has ended.

Privacy-by-design

- WeNet shall follow a privacy-by-design approach also with regard to the platform architecture.
- WeNet must guarantee privacy and data protection.
- WeNet shall ensure data protection through the appropriate privacy enhancing technologies and cryptographic methods.
- WeNet ensures that personal data is processed in a distributed and decentralised way.
- WeNet shall process personal data with the highest possible level of aggregation.

Monitoring and Iterated Evaluation

- WeNet shall develop a privacy policy for the RI, the platform and the application alike that is compliant with legal requirements and this privacy policy shall be enforced.
- WeNet shall implement internal procedures and policies aimed at securing compliance with data protection laws to help to facilitate ethical data handling [4].
- The set up of the platform shall be re-evaluated in reasonable intervals also from an ethical perspective and with particular care for privacy issues.
- WeNet shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet should consider the establishment of a standing techno-ethical committee that supervises the platform operations also with regard to privacy.

6.4 SMART UNIVERSITY PILOTS AND PRIVACY PROTECTION

WeNet conducts multiple pilots worldwide to continuously evaluate the WeNet platform. As a first step, critical topics in students' lives are identified. In a second step, scenarios are defined where WeNet services will be used. The scenarios are described through narrative techniques (user journeys). The scenarios will generate several technical requirements. Furthermore, data will be collected by means of field experiments carried out in several countries. Using convenience samples of university students, it aims at designing and validating instruments for diversity-measurement by means of survey and a prototype of a smartphone data collection tool. The WeNet services will be tested in various universities from the WeNet consortium through 4 waves of pilots. In the first iteration at M26 all the pilots will implement the same scenario: while the whole world is experiencing a global pandemic, a simple chat-bot tool that connects students otherwise isolated and far away from their campuses will be tested as a mean of re-connecting, provide help and support to each other. The evolution of the pilots is as follows:

Pilot at M26: this pilot will involve the students from the universities that participated in the diversity measurement pilots at M22-M24 (UNITN, AAU, LSE, NUM, UC, JLU). The aim of the pilot is to demonstrate that the platform can support the communication between participants in the "help me" scenario, integrating some basic features provided by the technical WPs. Furthermore, these pilots will provide more data to validate the model of diversity derived from the data collection at M22-M24 and will answer to specific research questions and hypotheses provided by the consortium.

Pilot at M32: this pilot will be an iteration of the previous one. For the first time though, the model of diversity will be implemented together with the needed algorithms to learn about individual and social practices and behaviours. The incentives and the norms will be further developed and implemented with respect to the previous pilot, updating also the research agenda of the various WPs. This will be the first pilot in which the students will be free to participate without any economic incentive: it is not a demonstrator but a functioning application with a value proposition in action.

Pilot at M34-36: this pilot aims at engaging with the community of innovators. The platform will be opened up to interested stakeholders that will exploit its features in their own context and with their own purposes and users. The aim is to demonstrate how flexible, robust and easy to use the platform is.

Pilot at M44: this will be the final iteration of the WeNet application. The details of this pilot will depend on the outcome of the previous ones. As a consortium we can imagine that the different universities involved in the pilots might decide on different directions: to keep the same scenarios of the pilot at M32 and iterate on it or to decide to explore different scenarios that might emerge from the data collected in the previous iterations. A decision about this will be taken after the analysis of the pilots at M32.

There will be also a formative evaluation parallel to the pilots on how to improve the service in the course of the project and a summative evaluation on the impact of the project on students' life, on universities and on communities that will run once the services provided by WeNet are tested.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Lawfulness

- Since WeNet carries out pilots in non-EU countries, particular attention shall be paid with regard to the lawful transfer of data from third countries.
- In the pilots in non-EU countries WeNet will nevertheless adhere to the legal requirements of the GDPR.

Transparency

- WeNet commits to transparency with regard to its data collection process in the pilots.
- WeNet shall provide its data subjects with information on the purposes of the processing.
- WeNet shall provide its data subjects with information on the categories of personal data concerned, that is what kind of data is collected.
- WeNet shall provide its data subjects with information on the recipients or categories of recipient to whom the personal data have been or will be disclosed.
- WeNet shall provide its data subjects, where possible with information on the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- WeNet will inform data subjects that it may store personal data for longer periods for achieving scientific research purposes.
- WeNet shall provide its data subjects with information on the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- WeNet shall provide its data subjects with information on the right to lodge a complaint with a supervisory authority.
- WeNet shall provide its data subjects with information on, where personal data are not collected from the data subject.
- WeNet shall provide its data subjects with any available information as to the source of the personal data collected.
- WeNet shall provide its data subjects with information on the existence of automated decision-making, including profiling.
- WeNet shall provide its data subjects with meaningful information about the logic involved in the automated decision-making, as well as the significance and the envisaged consequences of such processing for the data subject.
- WeNet shall provide the possibility for the data subjects to access their personal data.

Fairness

- The values inscribed in the scenarios in WeNet have to be constantly reflected with regard to their ethical aptness.
- Use case scenario design always runs the risk of stereotyping people, their needs and the means necessary to fulfil these needs. Therefore, WeNet shall pay utmost attention not to define stereotypical scenarios, so that no stereotypes are inscribed into the technology later on.
- Using convenience samples always run the risk of biases stemming from the selection mechanism. These possible biases have to be reflected in the research process and WeNet shall ensure that they do not lead to unfair discrimination.
- Students, although often and predominantly adults, are still relatively young and are still in a phase of education and orientation. Thus, they are in some ways to be considered as a vulnerable group. What is more: In pilots conducted by their universities they find themselves not on equal footing. It is a situation of power asymmetry and information asymmetry. WeNet shall pay due attention to this fact and treat these situations with due care.

Purpose Limitation

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet shall collect personal data only for the specified, explicit and legitimate purposes of the project and shall not further process them in a manner that is incompatible with those purposes.

Data Minimisation

- WeNet restricts data collection and processing to the least amount possible.
- Personal data collected during the pilots shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- WeNet shall ensure that the personal data collected during the various pilot activities is accurate and, where necessary, kept up to date.
- WeNet shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- WeNet shall respect the right to rectification that data subjects have both ethically and legally and the data subjects' right to obtain from the controller restriction of processing, if the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

Storage Limitation

- WeNet shall keep personal data in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. WeNet may store personal data for longer periods for achieving scientific research purposes.
- If WeNet stores data for longer periods, it shall implement the appropriate technical and organisational measures required in order to safeguard the rights and freedoms of the data subject.
- WeNet shall respect the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- WeNet shall respect the right of each data subject to obtain from the controller restriction of processing, if, though, the controller no longer needs the personal data for the purposes of the processing, but the data are required by the data subject for the establishment, exercise or defence of legal claims.

Data Security

- WeNet shall process data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

- WeNet appoints data controller to ensure accountability.
- WeNet shall set up procedures for handling complaints, reporting and responding to abuse with regard to privacy.
- When in doubt about legal standards and how to comply with regard to privacy but also in general, researchers will contact the WeNet management.

Protection of Minors

- WeNet is aware that amongst the student population there are also minors and it shall treat this fact with due consideration, since minors are particularly vulnerable to privacy

Co-funded by the Horizon 2020 Framework Programme of the European Union

threats and are often unaware how their digital footprint will affect them in the future.

Monitoring and Iterated Evaluation

- WeNet shall define and implement monitoring and evaluation procedures for the pilots with regard to privacy. These evaluation procedures shall be iterated over time. These can be formulated, for instance, in form of a “mission statement”.
- The formative evaluation on how to improve the services in the course of the project, shall include improvements with regard to privacy.

Enhancing Privacy Literacy

- WeNet shall take action to enhance privacy literacy among the students participating in the pilots.

6.5 WENET APP AND PRIVACY

WeNet designs a chatbot application to be used in the pilots and iteratively develops new features and functionalities according to the feedback from the piloting activities. The first WeNet application covers the “Getting answers/looking for 1 volunteer” use case. Such a chatbot application allows WeNet users to ask for information or for help to their peers. The app uses the resources and functionality exposed by the platform to provide users with a personalised experience based on diversity dimensions.[10].

Transparency

- WeNet commits to transparency with regard to its application design.
- The terms and conditions of the Smart University Application shall be formulated in an comprehensible way and they shall contain information on the following points.
- WeNet shall inform its data subjects and users of the various risks they face when interacting with the application.
- WeNet shall declare how and what data are managed and stored and who has access to these data.
- WeNet shall provide its data subjects with information on the categories of personal data concerned, that is what kind of data is collected.
- WeNet shall provide its data subjects with information on the recipients or categories of recipient to whom the personal data have been or will be disclosed.
- WeNet shall provide its data subjects, where possible with information on the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- WeNet will inform data subjects that it may store personal data for longer periods for achieving scientific research purposes.
- WeNet shall provide its data subjects with information on the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- WeNet shall provide its data subjects with information on the right to lodge a complaint with a supervisory authority.
- WeNet shall provide its data subjects with information on, where personal data are not collected from the data subject.
- WeNet shall provide its data subjects with any available information as to the source of the personal data collected.
- WeNet shall provide its data subjects with information on the existence of automated decision-making, including profiling.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet shall provide its data subjects with meaningful information about the logic involved in the automated decision-making, as well as the significance and the envisaged consequences of such processing for the data subject.
- WeNet shall provide the possibility for the data subjects to access their personal data.

Fairness

- The values inscribed in the set up of the application shall be constantly reflected with regard to their ethical aptness.
- WeNet shall ensure that data collected about individuals will not be used to unfairly discriminate against them.
- WeNet shall pay particular attention wherever there is a risk of stereotypes finding their way into the technical infrastructure. Furthermore, researchers in WeNet shall pay particular attention to situations, which involve particularly vulnerable groups, or power asymmetries or information asymmetries [4].

Purpose Limitation

- Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Further processing for achieving scientific research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data Minimisation

- WeNet restricts data collection and processing to the least amount possible.
- Personal data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- WeNet shall ensure that personal data processed via the application shall be accurate or respectively consistent with the authorized user data.
- WeNet shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- WeNet shall respect each data subject's right to rectification.
- WeNet shall respect each data subject's right to obtain from the controller restriction of processing, if the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

Data Security

- WeNet shall ensure that personal data is processed in a manner that provides appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- WeNet must guarantee privacy and data protection.
- WeNet shall ensure data protection through the appropriate privacy enhancing technologies and cryptographic methods.
- WeNet shall implement appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of pro-cessing systems and services.
- WeNet shall implement appropriate technical and organisational measures to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- WeNet shall process personal data with the highest possible level of aggregation.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Accountability

- WeNet shall name the contact persons for the Smart University Mobile App, in particular who is responsible for inquiries, complaints and with regard to liability law.
- WeNet shall set up procedures for handling complaints, reporting and responding to abuse with regard to privacy and the Smart University app.
- WeNet shall consider further oversight mechanisms to ensure privacy conducive data collection, storage, processing and use.

Privacy-by-design and by-default

- Respect for self-determination prohibits shifting one's own duties with reference to the free choice of the counterparty (e.g. transfer of the duty to protect privacy in possible incomprehensible terms and conditions to the free choice of the customer) [3]. WeNet shall follow a privacy-by-design and by-default approach with regard to the Smart University mobile application.
- WeNet ensures that in the application any personal data and their interrelationship are by default hidden from plain view.
- The Smart University application allows for various and diversified opt-in and opt-out possibilities with regard to privacy settings.
- When iteratively developing new features and functionalities according to the feedback from the piloting activities, developers shall reflect on in what way these new features and functionalities are conducive to privacy, or not – and adjust the implementation accordingly.

Protection of Minors

- Since minors may well be among the students participating in the pilots and using the Smart University Mobile app, appropriate steps must be taken to protect them accordingly. In any case, the app must have a registration restriction for people under 16.

Monitoring and Iterated Evaluation

- WeNet shall develop a privacy policy for the RI, the platform and the application alike that is compliant with legal requirements and this privacy policy shall be enforced.
- The Smart University App shall be re-evaluated in reasonable intervals also from an ethical perspective and with particular care for privacy issues.
- WeNet shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- WeNet shall implement internal procedures and policies aimed at securing compliance with data protection laws to help to facilitate ethical data handling [4].

Enhancing Privacy Literacy

- When iteratively developing new features and functionalities according to the feedback from the piloting activities, developers shall reflect on in what way these new features and functionalities are conducive to privacy literacy – and adjust the implementation accordingly.

6.6 DIVERSITY-AWARE LEARNING OF (ROUTINE) INDIVIDUAL BEHAVIOUR

With regard to diversity-aware learning of individual behavior WeNet will run two different levels of analysis: On the one hand from mobile sensor and log data to individual routines and then from individual routines to user categories. The input to the algorithms defined in WeNet are data streams provided by individuals through WeNet. The data used include time, location,

Co-funded by the Horizon 2020 Framework Programme of the European Union

social context as well as logs of interaction with the app itself. The output will feed the WeNet User Profiles. The Diversity-aware individual routine learning aspect of WeNet deploys probabilistic methods that are generalized to handle multiple data types and sources. As the data commons of WeNet grows due to multiple pilots and increased participation other methods that require more training data, for instance, deep learning methods will be assessed in terms of feasibility. In some cases diversity cannot be anticipated but could be learned from data. Therefore, WeNet deploys unsupervised and semi-supervised learning methods to discover non-predefined diversity-categories. The starting point, here, are nonparametric Bayesian models.WeNet employs unsupervised and semi-supervised learning methods.

From the perspective of the data and privacy protection the collection of personal data is of equal interest as the further processing of these data, more precisely the evaluation of the data and the possible transfer to third parties. Data protection also concerns data that the system itself generates through interaction with users [4]. From the perspective of data protection the analysis of behaviour patterns is also relevant.

Fairness

- The algorithms developed shall be fair and ensure that the machine mediation is not grounded in social stereotypes and biases that the machine learning inadvertently picks up from the learning data. Researchers in WeNet shall pay particular attention to situations, which involve particularly vulnerable groups, or power asymmetries or information asymmetries [4].
- The values inscribed in the algorithms shall be constantly reflected with regard to their ethical aptness.

Transparency

- WeNet discloses which aspects are powered by algorithms and lays out a concise description and explanation of the purpose of the algorithm; how it works and how it was trained; and what data it uses for its operation [10].
- WeNet shall provide its data subjects with meaningful information on the significance and the envisaged consequences of such processing for the data subject.
- The algorithms need to provide explanations about how and why routines are extracted in certain ways, including what data sources are used to extract routines and make algorithmic decisions.
- WeNet shall adhere the principle of “explicability” [12].
- If deep learning methods will be used in the future, it has to be ensured that their results are still interpretable for users, since interpretability is an important prerequisite for transparency.

Purpose Limitation

- Personal data shall not be further processed in a manner that is incompatible with the specified, explicit and legitimate purposes of their collection. Further processing for achieving scientific research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data Minimisation

- WeNet restricts data collection and processing to the least amount possible.
- Personal data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data security

- The algorithmic systems must guarantee privacy and data protection throughout a system’s entire lifecycle.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- Developers pay attention during programming, in the course of the development and monitoring of Machine Learning systems to defining and implementing sufficiently high security standards for the systems that suitably reflect different levels of criticality, taking into account different levels of autonomy, in order to minimise the risk of attacks.
- The algorithms shall as far as possible work with anonymised or pseudonymised data sets to prevent possible misuse.
- Developers working with personal data shall seek and be provided with technical training considering concepts such as differential privacy [3].

Monitoring and Iterated Evaluation

- All measures taken to protect data shall be reviewed and updated where necessary.
- The learning of routine behaviours shall be re-evaluated in reasonable intervals also from an ethical perspective and with particular care for privacy issues.
- WeNet shall implement internal procedures and policies aimed at securing compliance with data protection laws to help to facilitate ethical data handling [4].

6.7 DIVERSITY AWARE LEARNING OF SOCIAL RELATIONS

WeNet designs and implements socially-aware algorithms that learn the form and structure of social relations between users from streaming data of their social interactions: Thus, the algorithms continuously monitor the users and adapt to the possibly dynamic nature of their observed social interactions. They will accommodate for the diversity across users and social interactions considering the context or profile. The algorithms developed will be able to cope with missing information during training and deployment. They are, furthermore, fair in identifying social relations and ensure that machine mediation is grounded in the user's context and not in social stereotypes or biases that machine learning might pick up from the learning data.

To achieve these goals WeNet designs and implements learning algorithms, their underlying data structures, and associated inference mechanisms. These components are then be extended so that they can meaningfully be applied across different user contexts and different social interactions. In a further step, the developed components will be evaluated.

Fairness

- The algorithms developed shall be fair and ensure that the machine mediation is not grounded in social stereotypes and biases that the machine learning inadvertently picks up from the learning data. Researchers in WeNet shall pay particular attention to situations, which involve particularly vulnerable groups, or power asymmetries or information asymmetries [4].
- The values inscribed in the algorithms shall be constantly reflected with regard to their ethical aptness.

Transparency

- WeNet discloses which aspects are powered by learning algorithms. It also lays out a concise description and explanation of the purpose of the algorithm; how it works and how it was trained; and what data it uses for its operation [10].
- WeNet shall provide its data subjects with meaningful information on the significance and the envisaged consequences of such processing for the data subject.
- The algorithms need to provide explanations about how and why information on social relations are extracted in certain ways, including what data sources are used them and make algorithmic decisions.
- WeNet shall adhere the principle of "explicability" [12].

Co-funded by the Horizon 2020 Framework Programme of the European Union

Purpose Limitation

- Personal data shall not be further processed in a manner that is incompatible with the specified, explicit and legitimate purposes of their collection. Further processing for achieving scientific research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data Minimisation

- WeNet restricts data collection and processing to the least amount possible.
- Personal data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data security

- The algorithmic systems must guarantee privacy and data protection throughout a system's entire lifecycle.
- Developers pay attention during programming, in the course of the development and monitoring of Machine Learning systems to defining and implementing sufficiently high security standards for the systems that suitably reflect different levels of criticality, taking into account different levels of autonomy, in order to minimise the risk of attacks.
- The algorithms shall as far as possible work with anonymised or pseudonymised data sets to prevent possible misuse.
- Developers working with personal data shall seek and be provided with technical training considering concepts such as differential privacy [3].

Monitoring and Iterated Evaluation

- All measures taken to protect data shall be reviewed and updated where necessary.
- The learning of social relations shall be re-evaluated in reasonable intervals also from an ethical perspective and with particular care for privacy issues.
- WeNet shall implement internal procedures and policies aimed at securing compliance with data protection laws to help to facilitate ethical data handling [4].

6.8 PROFILES AND PRIVACY

WeNet carries out profile-building. The user profiles are used to perform profile matching. They will also allow contextual search capabilities as part of the interaction protocols. The profiles are based on Schematic Knowledge, Ground Knowledge and Streaming Knowledge. All three of them contain personal data. Thus, privacy-standards need to be met on all of the three Knowledge levels: Since the Schematic Knowledge level is structurally inspired by the habitus-theory of Bourdieu and data driven (consists of the analysis of survey data and app data), it is closely linked to the daily routines of the data subjects and very detailed. It contains highly personal data, for instance, with regard to a user's skills, material resources, practices and activities. The Ground Knowledge level contains a personal and a social profile. Both profiles contain, for instance, information on socio demographics. Additionally, the personal profile contains information on routines; the social profile information on social routines and practices. The Streaming Knowledge is based on data collected via physical and virtual sensors, time diaries, WeNet Interactions, online and offline interactions. It contains, for instance, contacts and agenda. The user profiles are used to perform profile matching. They will also allow contextual search capabilities as part of the interaction protocols.

Transparency

- WeNet shall disclose what types of information are extracted and abstracted on what grounds.
- WeNet shall disclose which entities, for instance which modules of WeNet, access this information.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet shall disclose, in particular, how and why routines are extracted in certain ways, including what data sources are used to extract routines.
- WeNet shall disclose how these data are then used to perform profile matching, for instance, on what grounds profiles are machted.
- WeNet shall provide information as to how to object to profiling, particularly in cases where data are inaccurate.
- WeNet shall provide its data subjects with information on the categories of personal data concerned, that is what kind of data is collected.
- WeNet shall provide its data subjects with information on the recipients or categories of recipient to whom the personal data have been or will be disclosed.
- WeNet shall provide its data subjects, where possible with information on the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- WeNet will inform data subjects that it may store personal data for longer periods for achieving scientific research purposes.
- WeNet shall provide its data subjects with information on the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- WeNet shall provide its data subjects with information on the right to lodge a complaint with a supervisory authority.
- WeNet shall provide its data subjects with information on, where personal data are not collected from the data subject.
- WeNet shall provide its data subjects with any available information as to the source of the personal data collected.
- WeNet shall provide its data subjects with information on the existence of automated decision-making, including profiling.
- WeNet shall provide its data subjects with meaningful information about the logic involved in the automated decision-making, as well as the significance and the envisaged consequences of such processing for the data subject.

Fairness

- WeNet has to ensure that it does not reinforce social stereotypes. Researchers in WeNet shall pay particular attention to situations, which involve particularly vulnerable groups, or power asymmetries or information asymmetries [4].
- The implicit normative assumptions in the data collection that feeds the profiling and the categories used will be constantly reflected with regard to their ethical aptness [14] [15] [16].

Purpose Limitation

- Personal data shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for achieving scientific research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data Minimisation

- WeNet restricts data collection and processing to the least amount possible.
- Personal data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

- WeNet shall ensure that personal data used for the profile building shall be accurate and, where necessary, kept up to date.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- WeNet shall respect each data subject's right to rectification.
- WeNet shall respect each data subject's right to obtain from the controller restriction of processing, if the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

Data Security

- WeNet must guarantee privacy and data protection.
- WeNet shall ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- WeNet shall ensure data protection through the appropriate privacy enhancing technologies and cryptographic methods.
- WeNet shall implement appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of pro-cessing systems and services.
- WeNet shall implement appropriate technical and organisational measures to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- WeNet shall process personal data with the highest possible level of aggregation.

Accountability

- WeNet will provide contact persons and complaint addresses for the data processing of the profiles.
- WeNet shall set up procedures for handling complaints, reporting and responding to abuse with regard to profile building.

Monitoring and Iterated Evaluation

- The profiling shall be re-evaluated in reasonable intervals also from an ethical perspective and with particular care for privacy issues.
- This re-evaluation shall be also used to implement practices that were not defined a priori and, thus, mitigate the risk of incorrectly profiling data subjects.

6.9 INCENTIVES DESIGN AND PRIVACY

WeNet will design algorithms and tools to generate diversity-aware incentives to maximize the probability of successful interactions. The research on incentive design relies on user models and social group models. Its efforts include policies for generating intelligent intervention messages that can sustain the engagement of diverse types of participants and virtual rewards for steering their behaviour towards desired outcomes for themselves and for the system. The approach taken here receives as input a training set of participant interaction histories collected in the first and second pilots as well – for preliminary work – datasets from volunteer-based crowdsourcing and questions-and-answer-sites. There will be incentives designed for single users as well as for multiple users. With regard to single users incentives design users will be segmented in "status classes" that reflect their contributions to the system. With regard to multiple users incentives WeNet will consider intervention messages which relate to users social behaviour, develop group formation algorithms for setting up "optimal working groups" and consider different badge designs (for instance quality and quantity-based badge types). Furthermore, diversity-aware badge placement will be considered and diversity-aware group formation based on historical data based on social interactions. There will also be a diversity-

Co-funded by the Horizon 2020 Framework Programme of the European Union

aware incentive-driven communication model developed for the interaction between humans and machines.

Transparency

- Increasing transparency is an important goal for personalization based systems [8].
- WeNet shall ensure that the data subjects are informed about the purpose of the personalization [8].
- WeNet shall inform the data subjects on why they receive certain incentives [8].
- WeNet shall disclose which data is used to create incentives [8].
- WeNet shall inform the data subjects about the pre-processing of the data that feeds the incentives [8].
- WeNet shall inform the data subjects about the behavioural models behind the incentives [8].
- WeNet researchers have developed a checklist for designers to evaluate and increase the transparency of their algorithmic systems. WeNet shall apply the principles formulated in the checklist to evaluate and increase the transparency of their algorithmic incentives systems (see Appendix).

Fairness

- The segmentation into “status classes” shall not unfairly discriminate data subjects.
- Users have to have the option to keep their status private.
- WeNet shall design non-addictive incentives. Incentives shall be designed in a way that does not hinder gaining an independent judgement on what to do.
- WeNet shall consider allowing data subjects to adjust timing and frequency of incentives [8].
- With regard to self-determination WeNet shall consider asking its data subjects about the goal for incentives for them and give them a say in the incentives design (“personalize the personalization”).

Data Minimization

- The incentives design and protocol shall try to use as little personal data as possible.

Accuracy

- The personal data used for the incentives shall be accurate. This is particular important with regard to the categorization in “status classes”.

Protection of Minors

- WeNet shall take it’s the special responsibility for minors seriously and choose a language that is appropriate for the protection of minors that may well be among the student population that uses the Smart University app in the pilots.
- In particular for children and minors it is of utmost importance to avoid addictive side-effects of incentives.

Monitoring and Iterated Evaluation

- WeNet shall implement a process for regularly testing, assessing and evaluating the incentives design and protocols in reasonable intervals.
- WeNet shall monitor the effect of the incentives design and try to spot addictive side-effects early on.

Enhancing Privacy Literacy

- WeNet shall consider implementing privacy literacy enhancing incentives (e.g. questions like: “Did you check your privacy settings recently?”)

Co-funded by the Horizon 2020 Framework Programme of the European Union

6.10 INTERACTION PROTOCOLS AND PRIVACY

WeNet develops and designs diversity-aware search mechanisms for matching profiles. To perform this search each person is associated a profile. As mentioned above parts of this profile are static others will contain real-time context and interaction context. Additionally, the profile will contain information about a persons past interactions. All of these aspects of the profile contain personal data and are, thus, relevant from a privacy perspective. A number of sample profiles will be designed in the process to accommodate different use cases. The interaction protocols have contextual search capabilities.

Transparency

- WeNet shall disclose on what grounds profiles are matched.
- WeNet shall disclose which data is used for the matching.
- WeNet shall inform the data subjects about the pre-processing of the data that feeds the interaction protocols.
- WeNet shall inform the data subjects about the models behind the matching process.

Fairness

- The interaction protocols developed shall be fair and ensure that the machine mediation is not grounded in unjust classifications.
- It must be ensured that data collected about individuals will not be used to unlawfully discriminate against them by WeNet and its various entities, particular with regard to the profile matching.
- Valuing the self-determination of its users WeNet will give its data subjects a say in the matching process.

Data Minimization

- The interaction protocols shall use as little personal data as possible.

Accuracy

- The personal data used for the profile matching shall be accurate.

Accountability

- WeNet shall set up procedures for handling complaints, reporting and responding to abuse with regard to matching and interacting with and via the platform.

Privacy-by-design and privacy-by-default

- WeNet shall follow a privacy-by-design and a privacy-by-default approach with regard to the interaction protocols. This is in particular important with regard to the contextual search capabilities and the possible privacy infringements and according misuse scenarios in the offline world.

Protection of Minors

- At this development stage it can not be ruled out that activities inappropriate or illegal for minors are proposed via a WeNet application. WeNet has to implement appropriate means for the protection of minors with regard to these activities. Options may include not matching minors for such activities, labelling these activities as not age-appropriate etc. WeNet shall in any case define a list of activities that fall under this category and procedures of how and when to update this list.

Monitoring and Iterated Evaluation

- The workings of the interaction protocols shall be monitored and evaluated in reasonable intervals.

Co-funded by the Horizon 2020 Framework Programme of the European Union

6.11 OPEN ONLINE COURSE AND PRIVACY

WeNet will make online educational, tutorial and training material available to facilitate uptake of the project outcomes by newcomers. WeNet will produce educational videos and materials that explain the WeNet vision and its enabling technologies. The educational material will form a complete Open Online Course with an introductory and two parallel complementary tracks for researchers and developers. These Tracks will cover WeNet's basic notions (Track 1), the WeNet Research Infrastructure (Track 2), and the WeNet platform (Track 3). The two main tracks (1 and 2) aim to motivate the learner to study how to generate data to understand human behaviour using the WeNet Research Infrastructure and how to develop WeNet compliant apps using the WeNet platform.

The Wenet eLearning Platform also hosts, as mentioned above, the Data Protection Forum (DPF, see 1.3.). Participants can watch the short videos for introducing the DPF and get background information on privacy and data protection. These videos address ethical questions and present principles of data ethics, which are also inscribed in the EU General Data Protection Regulation (GDPR). Participants can join the forum and start a discussion or reply to discussions initiated by other users.

The online course is delivered through the WeNet eLearning platform, which offers tools for users to read the data protection policy, preview all personal data held by the platform for them and choose to erase their data and account at any time..

Transparency

- WeNet shall provide the participants of the Open Online Course information regarding the way in which data is collected, evaluated and used.

Fairness

- It must be ensured that data collected about individuals will not be used to unlawfully discriminate against them by WeNet and its various entities.
- The values inscribed in the set up of the online course and its evaluation methods have to be constantly reflected with regard to their ethical aptness.
- Since the online course will hand out certificates, it needs to be monitored whether some participants are unfairly disadvantaged by the set up of the course.

Enhancing Privacy Literacy

- WeNet will develop tools and online courses to support data literacy in general but also to support its platform users to become competent users [10] with regard to privacy. The Open Online Course shall cover topics that are conducive to privacy literacy.

6.12 ETHICS AND PRIVACY

As mentioned above, WeNet follows an integrated research approach, thus, ethical reflection and consideration is a task for all project partner. The ethics partner, however, has a special responsibility to raise awareness to all ethical issues that emerge in the project and provide guidance as to how to approach them.

Fairness

- All partners will constantly reflect on the values inscribed in the technological tools, services, and algorithms developed in WeNet and their ethical implications. The ethics partner will provide guidance and methods with regard to these reflection processes. It will facilitate conversations and discussions on privacy with all partners. An important instrument for these discussions is theDPF.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- WeNet shall pay utmost attention to the categories and scenarios it uses during its various research, development and design phases and shall avoid stereotyping and discrimination.
- The conceptual framework for diversity shall lay the foundations for a non-discriminatory approach to diversity in WeNet.
- All partners shall raise awareness whenever data collected in the research process runs the risk to be used for discriminatory purposes.
- WeNet's assessment of potential of misuse scenarios shall include but is not limited to threats to data privacy, protection of minors, threats to fairness and transparency.

Monitoring and Iterated Evaluation

- It shall be monitored whether ethical issues emerging in the research process are handled with due care and consideration.
- Privacy is a core value for WeNet's ethical management. The ethics partner will raise awareness to possible violations of privacy-standards and facilitate discussions on matters such as privacy from an ethics perspective.
- The ethics partner of WeNet offers to double-check all processes and procedures for their ethical compliance.
- The ethics partner shall provide expertise on possible threats to privacy in WeNet.

Enhancing Privacy Literacy

- Researchers from the ethics partner shall as all others partner try to enhance privacy literacy amongst students as well as the general public through their teaching, participation in workshops and conferences raising attention to privacy issues as well as other activities to that purpose.

6.13 DISSEMINATION

WeNet has its own Website and uses social media channels (i.e. Twitter, Linkedin, Youtube). It disseminates its results through publications and presentations at conferences, workshops and relevant scientific, industrial and EC-driven events. WeNet activities includes the organization of two engagement workshops aiming at involving local communities for effective participation to the pilots and two policy workshops on the implications of the WeNet vision and outcomes for policy makers. The project also organizes the first of a series of new interdisciplinary conferences in empowering machine-mediated diversity-aware interactions.

Privacy-by-design and by-default

- WeNet shall use a privacy-as-default approach with regard to the privacy-settings of its own website.

Enhancing Privacy Literacy

- WeNet shall use its Website and social media channels where possible also to share information on privacy literacy and engage in privacy literacy enhancing activities.
- WeNet researchers should, where this appears suitable, consider attending and engaging in conferences, events and workshops on privacy literacy.
- WeNet researcher should consider publishing on matters of privacy literacy, or should address matters of privacy literacy in their publications into account where relevant.
- WeNet's policy workshop should also address questions of privacy literacy.

Co-funded by the Horizon 2020 Framework Programme of the European Union

7. CONCLUSIONS

Development and application of technology are never value-neutral processes. Rather, they are embedded in a framework of ethical and social values and principles which are inscribed into technology, but which are also influenced by technology.

WeNet with its various technological components, which is still in an early stage in some areas, is no exception. On the contrary: A platform and research infrastructure on the basis of which a diversity-aware machine mediated paradigm for social relations and interactions is to be developed represents a great challenge from an ethical perspective for principles of self-determination and privacy due to its special characteristics.

Privacy and self-determination are fundamental elements of liberal and democratic societies. Therefore, the integration of ethical principles is of central importance in the development of such a platform and research infrastructure. In this task, the actors who develop and refine the various technical elements in WeNet bear a particular responsibility: They have to ensure that ethical values and principles (e.g. transparency, fairness, and accountability) are observed during the development and design phase and by the technology itself.

In this deliverable, we outlined a guideline that further develops WeNet's threefold approach to privacy protection: The guideline proceeds on the assumption of lawfulness of all activities in WeNet. Privacy-by-design and by-default are its guiding principles when it comes to the technological implementation of data protection and privacy. Acknowledging the fact that WeNet works in an evolving and highly dynamic field of research, that gives raise to new and unforeseen questions also regarding privacy and data protection, WeNet has launched the WeNet Data Protection Forum (DPF) to provide a venue to discuss these questions and find solutions for them together.

Based on these three elements of privacy and data protection WeNet had formulated a preliminary guideline concerning privacy-standards for WeNet. Since the publication of the first preliminary guideline research in WeNet and on privacy in general has evolved, thus making certain specifications and further considerations concerning the relation between diversity and privacy, responsibility for privacy and privacy literacy sensible.

It was, thus, stressed that a diversity-aware machine mediated paradigm for social relations and interactions processes sensitive personal data and, thus, has to put particular emphasis on privacy protection to not leave its data subjects vulnerable to various misuse scenarios leading to privacy infringements and harm. Furthermore, since diversity dimensions are fluid and context-dependent and, thus, independent control for users of how they are represented on a platform is particularly important, a contextual and non-static understanding of privacy is needed that allows for different spheres of privacy that are guided by different norms for the interaction and information flows that take place in them.

In a complex technological development and research structure as WeNet the implementation of privacy norms needs the effort of all partners involved. What is, thus needed, is a multidimensional and proactive understanding of responsibility that entails (but is not limited to) notions professional, framework and user responsibility.

To enable users and data subjects to act responsibly with regard to privacy, the enhancement of privacy literacy among the students participating in the project as well as in general is imperative. WeNet researchers engage in various activities to empower data subjects to use digital media, digital platforms and services in such a way that their own privacy is protected. Privacy literacy, however, is not regarded as a general solution, because it does come with a number of problems that need to be acknowledged.

Co-funded by the Horizon 2020
Framework Programme of the European Union

The revised and amended privacy-guideline is based on the following general principles: transparency, fairness, purpose limitation, data minimisation, accuracy, storage limitation, data security, accountability, privacy-by-design and by-default, protection of minors, monitoring on a regular basis and iterated evaluation as well as support of privacy-literacy. These general principles were, then, applied to all central components of the WeNet research project.

The guideline, however, is not providing legal advice or guiding on how to achieve compliance with existing legal norms and requirements concerning privacy-standards. It provides ethical guidance with regard to privacy and on how to implement abstract ethical principles into concrete measures.

Co-funded by the Horizon 2020
Framework Programme of the European Union

REFERENCES

[1] Reinhardt, K. et al. (2019): A Preliminary Guideline Concerning Privacy-Standards for WeNet, available online: https://www.internetofus.eu/download/d9-2-a-preliminary-guideline-concerning-privacy-standards-for-wenet/?wpdmdl=943&masterkey=5e2af83345314, last checked on 04/12/2020.

[2] European Data Protection Supervisor (2015): Towards a new digital ethics. Data, Dignity and technology, available online: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf, last checked on 04/12/2020.

[3] Heesen, J. et al. (Hrsg.): Ethik-Briefing. Leitfaden für eine verantwortungsvolle Entwicklung und Anwendung von KI-Systemen – Whitepaper aus der Plattform Lernende Systeme, München 2020.

[4] AI High Level Expert Group (2019): Ethics Guidelines for Trustworthy AI, Brussels.

[5] Grimm, P./ Krah, H. (2016): "Privatsphäre", in: Jessica Heesen (ed.): Handbuch Medien- und Informationsethik, Stuttgart, pp. 178-185.

[6] Hagendorff, T. (2018): Privacy Literacy and Its Problems, in: *Journal of Information Ethics* 27 (2), pp. 127–145.

[7] Cavoukian, A. (2011): Privacy by design. The 7 foundational principles, available online: www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf, last checked on 04/12/2020.

[8] Hoepman JH. (2014): Privacy Design Strategies, in: Cuppens-Boulahia, N. et al. (eds): ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology, vol 428. Springer, Berlin, Heidelberg, pp. 446-459.

[9] Schelenz, L. et al. (2020). Best Practices for Transparency in Machine Generated Personalization, in: *Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization* (*UMAP '20 Adjunct*). Association for Computing Machinery, New York, NY, USA, pp. 23–28.

[10] Hartford, M. et al. (2016): A Social Charter for Smart Platforms, available online: https://eprints.soton.ac.uk/410307/1/SmartSocietySocialCharterforSmartPlatforms_final.pdf, last checked on 04/12/2019.

[11] Rosell, B. et al. (2020): WeNet Platform and Research Infrastructure, available online: https://www.internetofus.eu/download/d6-1-wenet-platform-architecture-specifications/?wpdmdl=1221&masterkey=5ede23e2d263f, last checked on 04/12/2020.

[12] Floridi, L. et al. (2018): AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, in: *Minds and Machines* (28), pp. 689-707.

[13] Zech, H. (2019): Liability for autonomous systems: Tackling specific risks of modern IT, in: *Lohsse/Schulze/ Staudenmayer* (Hrsg.), Münster Colloquia on EU Law and the Digital Economy IV, Liability for Artificial Intelligence and the Internet of Things, Baden-Baden, pp. 185-200.

Co-funded by the Horizon 2020 Framework Programme of the European Union

[14] Schelenz, L. et al. (2019): Developing a conceptual and ethical framework for modelling diversity, available online: https://www.internetofus.eu/download/d9-1-ekut-ethical-framework/?wpdmdl=651&masterkey=5d415920a3f1e, last checked on: 02/12/2020.

[15] Reinhardt, K. (2020): Between Identity and Ambiguity. Some Conceptual Considerations on Diversity, in: *Symposion* 7 (2), pp. 261-283.

[16] Heesen, J. (2021): Diskriminierung durch Algorithmen vermeiden. Analysen und Instrumente für eine demokratische digitale Gesellschaft, in: G. Bauer et al. (eds.): Diskriminierung und Anti-Diskriminierung. Beiträge aus Wissenschaft und Praxis, Bielefeld, S. 127-145 (forthcoming).

[17] Nissenbaum, H. (2019): Contextual Integrity Up and Down the Data Food Chain, in: 20 *Theoretical Inquiries in Law* 20, pp. 221-256.

Co-funded by the Horizon 2020
Framework Programme of the European Union

APPENDIX

FIGURE 5: TRANSPARENCY CHECKLIST SCHELENZ ET AL. (2020)

General:
Does the system inform the user about the purpose of personalization?
Does the system inform the user who developed the technology and is liable in cases of wrongdoing?
Does the system inform the user about their rights under data protection law?
Does the system inform the user about possible risks of engaging with the system?
Input:
Have users given informed consent about the collection, processing, and storage of their data?
Does the system inform the user about the fact that data is collected for personalization?
Does the system inform the user about which data is collected to produce personalized content for them?
Does the system inform the user about pre-processing done with the data collected for personalization purposes?
Does the system inform the user if their data is used and shared beyond the goals of personalization?
Processing:
Does the system inform the user about the kind of data that is processed to create a certain personalized item?
Does the system explain to the user why they are receiving a certain personalization?
Does the system inform the user about the behavioral models underlying the personalization system?
Does the system inform the user about possible constraints of the model such that may result from pre-processing or biases in the dataset?
Output:
Does the system present information to the user in a location where they can notice it and access it easily?
Does the system provide information to the user in a comprehensible way and can they act upon this information?
Does the system provide the user with information in a clear and simple language that avoids technical terms?
Does the system make it clear to the user that they interact with a machine?
Control:
Does the system provide the user with the opportunity to specify their goals which are then used for personalization?
Does the system provide the user with different options as to the personalized content they receive?
Does the system provide the user with opt-in and opt-out options (e.g. for data collection)?
If applicable, can the user adjust frequency and timing of personalized content?
Does the user have a say in which data or models are used for personalization?
Does the system encourage the user to give feedback and express their opinion about the personalization mechanisms used (type, frequency, duration, etc.)?

Table 2: Transparency Checklist

Co-funded by the Horizon 2020 Framework Programme of the European Union