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

D9.2 A PRELIMINARY GUIDELINE CONCERNING PRIVACY-STANDARDS FOR WENET

Revision: v.1.0

Work package	WP 9
Task	9.2
Due date	31/12/2019
Submission date	18/12/2019
Deliverable lead	EKUT
Version	1.0
Authors	Dr. Karoline Reinhardt (EKUT), Laura Schelenz (EKUT), PD Dr. Jessica Heesen (EKUT), Andreas Baur (EKUT)
Reviewers	Daniele Miorandi (UH)

Abstract	The GDPR asks for various forms of privacy protection: In many ways its proposed privacy by and in design as well as by default approach is not only a legal standard but also a claim for many ethical concepts for data security and privacy protection in the digital world. In this deliverable, we distinguish three forms of privacy and explain the value of privacy with regard to the individuals as well as societies as a whole. We will lay out the notion of privacy of the GDPR and propose a "privacy by design"-approach. We will go on to describe measures that are currently taken in WeNet to protect users' data and adhere to legal and ethical principles of privacy enhancement. The deliverable will also introduce the WeNet Data Protection Forum, an institutionalized discussion forum, where researchers and developers in WeNet can debate and resolve questions of data protection. Building on the findings of the previous sections, the deliverable formulates a preliminary guideline concerning privacy standards for WeNet.
Keywords	privacy, data protection, ethics, values

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	09/10/2019	1st draft	Karoline Reinhardt (EKUT)
V0.2	26/11/2019	2nd draft	Karoline Reinhardt (EKUT), Laura Schelenz (EKUT)
V0.3	02/12/2019	internal revision	Karoline Reinhardt (EKUT), Laura Schelenz (EKUT), Jessica Heesen (EKUT), Andreas Baur (EKUT)
V1.0	17/12/2019	final version	Karoline Reinhardt (EKUT), Laura Schelenz (EKUT), Jessica Heesen (EKUT), Andreas Baur (EKUT)

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

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

The GDPR asks for various forms of privacy protection: In many ways its proposed privacy by and in design as well as by default approach is not only a legal standard but also a claim for many ethical concepts for data security and privacy protection in the digital world. However, with regard to the manifold possible threats to privacy it is not enough to adhere to the legal standards alone but also to think ahead.

The WeNet consortium is aware that a platform that is diversity-aware is also dealing with particularly sensitive data. A software application that works with data relevant to diversity carries a considerable responsibility towards the protection of its users' data. It also carries a considerable risk of losing control: When people reveal information about individual problems and look for help in a diverse community, there is a risk that people with harmful intentions might exploit it.

Therefore, data and privacy protection play a crucial role within the WeNet project.

In this deliverable, we distinguish three forms of privacy – decisional privacy, locational privacy and informational privacy – and explain the value of privacy with regard to the individuals as well as societies as a whole. Privacy enables us to make decisions free from interference and manipulation. It allows us to formulate life plans. This is particularly important in democratic societies, where democratic processes rely on the free expression of diverse opinions.

We will then lay out the notion of privacy of the GDPR, the principles for data protection it states, the rights of data subjects it formulates, and the responsibilities and obligations it derives from these.

After that, we will propose the "privacy by design"-approach as a possible solution, state its seven principles and formulate eight possible strategies for technology design that can be derived from these principles and will help to implement the privacy by design approach.

We will go on to describe measures that are currently taken in WeNet to protect users' data and adhere to legal and ethical principles of privacy enhancement. Among these measures are the ethical approval of all experiments and pilot trials by local experts, informed consent, data protection impact assessment, transparency with regard to research purposes, and technical measures affecting the user profile, the security of the server, and pseudonymization/anonymization. The deliverable will also introduce the WeNet Data Protection Forum, an institutionalized discussion forum, where researchers and developers in WeNet can debate and resolve questions of data protection. We will propose some key issues that may be taken up by the forum in the future. These issues include a possible "mission statement" with regard to research purposes, questions around data ownership and empowering the user, the sustainable use of data generated in the WeNet project, as well as ethics guidelines for platform operators and app owners.

Finally, and building on the findings of the previous sections, the deliverable formulates a preliminary guideline concerning privacy standards for WeNet.

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

ABBREVIATIONS

DPIA	Data Protection Impact Assessment
EKUT	Eberhard Karls Universität Tübingen
GDPR	General Data Protection Regulation of the European Union
PbD	Privacy by Design
PET	Privacy Enhancing Technologies
UH	U-Hopper
WP	Work package

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

1. INTRODUCTION

"In today's digital environment, adherence to law is not enough; we have to consider the ethical dimension of data processing" (European Data Protection Supervisor 2015, 4)

WeNet aims at developing an end-to-end people network that will be aware and robust to all forms of diversity among people. The project consortium is aware that some ethical, fundamental rights, privacy and data protection issues are raised by designing and developing a general-purpose application-independent people interaction protocol. The role of ethics, therefore, plays a crucial role in this project.

Privacy is one of the main relevant ethical topics of the WeNet project: A software application that works with data relevant to diversity carries a considerable responsibility towards the protection of its users' data. It also carries a considerable risk of losing control: When people reveal information about individual problems and look for help in a diverse community, there is a risk that people with harmful intentions might exploit it.

Five different respects can be identified in which the protection of data privacy is in jeopardy in electronic databases:

1) Reliability: In an open communication infrastructure, the trustworthiness and competence of data collectors cannot be ensured.

2) Ungovernable diffusion: If data are in an external database system or on the Internet, it is possible to gain control over their further use. On the one hand, there is a threat for data to be sold to shady vendors; on the other hand, once information has been propagated in many different files, it is difficult to eliminate or even to modify data.

3) Data mining: There is a high potential for combining data in systematic ways to create detailed, composite profiles of individuals.

4) Identity theft: Digital identities can be misused, for example, for credit card fraud or even to damage personal identity by using it for wrong or denunciatory websites.

5) Malicious attacks: Data management systems are predominantly ineffectively defended from criminal hacking or aggression in information warfare.

Liberal social orders place high significance on the protection of the private sphere, especially because the safeguarding of a private sphere is a necessary precondition for the protection of the freedom of action. Only in a realm that is extensively protected from heteronymous conditions can that spontaneity and unbiased behaviour be cultivated, which is tied to the concept of freedom of action and self-fulfilment. The concept of privacy also provides protection against discrimination and is an important feature of non-discriminatory policies. Furthermore, dividing society into various societal spheres and contexts helps to prevent totalitarian regimes.

The concept of privacy concerns the exclusion of various persons or groups from knowing certain aspects or data from an individual's life. From an individual perspective, the protection of privacy is associated with the control of information, spaces, or property. That is not to say that it is about secrecy, but rather about contextual integrity (Nissenbaum 2010). Contextual integrity means that privacy is provided by appropriate information flows. The appropriateness of information flows is defined by the norms of each context with regard to information. In this sense, privacy is a supporting condition and part of a person's agency.

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

Three forms of privacy are commonly distinguished: (1) decisional privacy, (2) local and spatial privacy and (3) informational privacy (cf. Heesen 2012, 541; Rössler 2001). All three forms of privacy are relevant to WeNet. Informational privacy being probably the most obvious one.

Informational privacy refers to the protection and control of personal data. It is understood as "the ability if individuals to have control and freedom about the collection, use and disclosure of information about ourselves" (Cavoukian 2012, 3). In datafied societies like the ones we live in, informational privacy is the "supreme discipline" of privacy since it concerns all aspects of our lives – and since the other forms of privacy also have informational aspects.

WeNet, on top of this, also deals with issues concerning decisional privacy and local and locational privacy:

Decisions are increasingly made as a reflection of the reaction to a technological system. The knowledge that data on individual behaviour are being collected and the simultaneous non-transparency of which data exactly are collected at what moment in time effects the decisions people make and how they behave.[1] There are effects of surveillance like self-discipline and self-censorship that strongly impair the free development of the individual. These effects are also known as "panoptism" (cf. Foucault 1975). The WeNet application will also through incentives affect the decision process of its users. In this way WeNet acts as a 'persuasive technology' in order to stimulate pro social behaviour. WeNet has to ensure that this does not result in "panoptic effects".[2]

With regard to locational privacy, we note that systems that create and store data on people's movements have become a part of our everyday life. WeNet will not be an exception to this. It will also collect and process data that are concerned with the whereabouts of people and their movement. This carries an overt risk of misuse, but also of hidden side-effects of in other regards useful services.

These risks and threats to privacy place a special responsibility on developers, programmers, designers, data controllers and data processors with regard to the protection of privacy.

We will propose a privacy by design and by default approach as developed by John Borking and Ann Cavoukian and formulate a preliminary guideline for WeNet that applies the principles and strategies of a privacy by design approach to the research process in WeNet as well as the actual WeNet platform and application.

However, determining private spheres and data differs in the given sociohistorical and cultural context and, accordingly, the individual roles at play. A platform like WeNet that wants to place special consideration on diversity has to be aware of this and needs to find according solutions.

In this deliverable, we will start from the notion of privacy of the GDPR and propose a "privacy by design"-approach. We will, then, go on to describe measures that are currently taken in WeNet to protect the privacy of the data subjects and the users. The deliverable will also introduce the WeNet Data Protection Forum, an institutionalized discussion forum, where researchers and developers in WeNet can debate and resolve questions of data protection. Building on the findings of the previous sections, the deliverable formulates a preliminary guideline concerning privacy standards for WeNet.

Though, in this deliverable, we rely heavily on legal literature on matters of privacy, we are not proposing a legal opinion but an ethical argument about privacy and its protection.

[1] On the relation of trust and transparency on the Web also cf. Simon (2010).
[2] On the concept of decisional privacy see also Floridi (1999 and 2006).

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

2.WHY PRIVACY?

Given the increased relevance of questions of data privacy and data protection, this section will remind readers of why we value and pursue privacy and data protection. Privacy is important to realize our life plans and be the person we want to be. It directly relates to personal autonomy, identity, and the self. Privacy helps us grow personally and develop our character and ourselves (Rössler 2001). In the tradition of liberalism, privacy is valued because it allows societies to realize democracy and pluralism. Only when individuals are protected from state interference or manipulation, they are free to express their interests and put their preferences into action (Rawls 2005; Westin 2015). Similarly, we value data protection because control over our own data means that we are potentially less exposed to manipulation and discrimination. If information is available about ourselves, it may be used to exploit our vulnerabilities and align our interests with third party interests (Susser et al. 2018).

Hence, we can make three arguments for privacy, which are interrelated and reinforce one another: 1) privacy is a prerequisite for personal autonomy; 2) (data) privacy is crucial for democracy; 3) data privacy protects us from unwanted interference and thus fosters free decision-making. These three arguments reflect Western liberal attitudes towards privacy and individual autonomy. However, privacy is a normative concept and can have different interpretations depending on the cultural context. In intercultural information ethics, the significance and impact of different concepts of privacy is much discussed. Some cultural traditions stress the importance of community for personal identity. Accordingly, privacy can also have negative connotations. For instance, in some cultures, privacy has traditionally been considered shameful and suspicious, as a claim to privacy seems like a person wants to hide something bad from the community or society (Ess 2005; Capurro 2005). Understanding these different philosophical and cultural traditions is important because they inform the data protection regimes in the respective countries. They also stress that the value of privacy as laid out below is bound by its underlying Western liberal assumptions and worldviews. Besides, even within the Western context, we can see differences in interpretations of privacy, for instance between the United States and Europe (Rössler 2001, 33ff.).[3]

Privacy (in a functional sense) is a prerequisite for personal self-determination (Rössler 2001, 95). In order to be an autonomous person and determine one's life path, someone needs a private space to develop ideas, beliefs, and plans. This means that the person has control over access to this private space (symbolically or physically). The person must be able to control their relationship to themselves, to specified others, and to random other people. These relationships (whether intimate or otherwise) require privacy in order to be developed. When my privacy is violated, it follows that I have no full opportunity to develop these constitutive relationships and my autonomy may be compromised (Rössler 2001, 127ff). In the context of informational privacy or data protection, individuals accordingly need control over who has access to their information (Rössler 2001, 201ff). However, there are limitations to the idea that full control fosters autonomy. For instance, giving a user more control might be counterproductive, if the user does not know how to make good of it (Friedman and Nissenbaum 1996).

Data privacy is also crucial for realizing democracy. Freedom of expression, the formation of multiple political positions, and social participation is only possible if individuals are free from state suppression or coercion (Rawls 2005; Habermas 1990; Westin 2015; Davis and Kelley 2012). Some challenges to democracy arise from the emergence of digital worlds and fora for (political) engagement online. For instance, the use of big data analysis and quantified information for policy-making raises concern about a possible technocracy. Big data can be scraped and analyzed (often without the awareness of users) to create policies and promote new services. There is no doubt that it makes sense to use empirical and general scientific

[3] Please see a more extensive chapter on "Privacy Across Cultures" in the WeNet Deliverable 11.2.

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

knowledge for political processes and decisions. How else could one come to an informed decision? Despite this, the advanced forms of data analysis develop their own dynamics that connect to the past lines of discussion about technocracy (cf. Heesen 2016, 18). It is therefore critical that users are aware of the potential uses of their data and can potentially adjust their behavior.

Finally, privacy and data protection shield individuals from manipulation that restrain their freedom of choice and decision-making. This concern relates to the right to decisional privacy. Especially in the context of social media, person-related data is used to promote or withdraw certain content from users. This has implications for users' ability to make independent choices. Online manipulation can be defined as "the use of information technology to covertly influence another person's decision-making" (Susser et al. 2018, 24f). This means that manipulation, other than persuasion and coercion, is conducted in a subtle, hidden way. Manipulation usually plays on the beliefs, desires, and emotions of people and exploits their vulnerabilities to achieve a certain end. In the context of voting and democratic decision-making processes, the exposure to manipulation due to lack of privacy can have serious implications. Data protection thus protects users' ability to conduct themselves autonomously in a democratic society.

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

3.PERSONAL DATA AND PRIVACY BY DESIGN

3.1. GDPR AND PERSONAL DATA

3.1.1. Definitions

Article 4 of the General Data Protection Regulation (GDPR) states the important definitions with regard to personal data, including among others collection, storage, dissemination of personal data.

Personal data are defined as „any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (article 4.1 GDPR).

According to article 4.2 processing "means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.".

The restriction of processing is then in article 4.3 defined as „the marking of stored personal data with the aim of limiting their processing in the future".

"Profiling" means, according to article 4.4, „any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

Article 4.11 defines how we ought to understand 'consent' according to the GDPR: „any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Article 5 of the GDPR then defines the conditions for consent:

„Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

1. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

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

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

With regard to children special consideration needs to be given: According to article 6.1, "where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child."[4]

3.1.2. Principles relating to processing of personal data

Article 5 GDPR states principles related to the processing of personal data: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability:

1. Lawfulness, Fairness, Transparency

personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

2. 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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes;

3. Data Minimisation

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

4. 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;

5. 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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;

6. Integrity and Confidentiality

[4] WeNet has described its privacy operating procedure in an internal project document prepared and distributed by WP11.

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

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.

7. Accountability

The data controller is responsible for the compliance with the stated principles and shall be able to demonstrate this compliance.

3.1.3. Rights of the data subject

From these principles follow, according to articles 12-23 GDPR, the following rights of the data subject:

1. Right to transparent information (art. 12)

2. Right to information on where personal data are collected from the data subject (art. 13)

3. Right to information on where personal data have not been obtained from the data subject (art. 14)

4. Right to access by the data subject (art. 15)

5. Right to rectification (art. 16)

6. Right to erasure ("right to be forgotten") (art. 17)

7. Right to restriction of processing (art. 18)

8. Right to data portability (art. 20)

9. Right to object (art. 21)

10. Right not to be subject to a decision based solely on automated processing, which produces legal effects (art. 22)

3.1.4. Responsibilities of Controller and Processor

As mentioned before, the data controller is responsible for the compliance with the stated principles and shall be able to demonstrate this compliance (accountability). Art. 24 of the GDPR states:

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

These measures include but are not limited to "measures, such pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects" (art. 25).

"The controller" furthermore "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each spe-

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

cific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." (ibid.)

With regard to the responsibilities of the data processor the GDPR states: "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject" (art. 26). The data processor „shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law" (art. 29).

A further responsibility concerns the records of processing activities: "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility" (art. 30). The content of these records is specified in art. 30.1 a-f.

"The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing" (art. 32).

Article 33 and 34 deal with personal data breaches as defined above: „In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." It falls also within the responsibility of the data controller to „communicate the personal data breach to the data subject without undue delay", in cases where "the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (art. 34)

Special consideration is warranted, where "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data" (art. 35).[5]

3.2.PRIVACY BY DESIGN AND BY DEFAULT

[5] For the technical and organizational measures that will be implemented: WeNet Deliverable (D 11.2.).

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

3.2.1. Why Privacy by Design?

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

Furthermore, Ann Cavoukian, the then Canadian Information & Privacy Commissioner, published the concept of privacy by design in the 1990s and thereby extended the idea of privacy enhancing technologies to include positive values. She formulated seven foundational principles of privacy by design that should be followed not only in the development of technology, but also in the organisation of businesses and practices. She argues: 'Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation' (Cavoukian et al. 2010).

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

Article 25.1 GDPR states: „Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

Article 25.2 GDPR explains the responsibilities of the controller: „The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

3.2.2. Principles of Privacy by Design

The foundational principles of privacy by design, according to Ann Cavoukian (2011), are:

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

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

"3. Privacy Embedded into Design"

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

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

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

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

"6. Visibility and Transparency – Accountability, Openness, Compliance"
Assure all users and stakeholders that the system is working according to the stated promises and objectives. Make independent verification possible by keeping all components and processes visible and transparent.

"7. Respect for User Privacy – Consent, Accuracy, Access, Compliance"
Respect the interest of the individual uppermost. Keep it user-centric, make privacy the default, notice the individual when needed and empower user-friendly options.

3.2.3. Privacy Design Strategies

Eight privacy design strategies can be derived from a privacy by design approach following Jaap-Henk Hoepman (2014, 452-457) that will help to implement the principles:

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

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

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

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

5. INFORM
Every time an individual uses a data processing system, the user should be informed about what data is processed, for what purpose and how. And also, how it is protected and who

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

has access to this information. Moreover, data subjects should be provided with information about their access and deletion rights. This helps to ensure openness and transparency.

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

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

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

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

4. WENET AND PRIVACY

4.1. EFFORTS OF THE CONSORTIUM

While WeNet is still in its initial phase of the project with regard to the development of the WeNet application, where data collection processes are designed and the research infrastructure is built, WeNet has already laid out important steps towards protecting the privacy of data subjects in the pilots and envisioned WeNet users. These measures are described in this section. They are complemented by a list of open questions and topics with regard to data protection in WeNet that should be discussed and if necessary and helpful, pursued in the following years. The information provided in this section relies on personal interviews with WeNet partners in charge of designing data protection measures for the pilot trials (i.e. data collection and subsequent processing of data) and the architecture and technical realization of the WeNet platform.

Ethical approval of experiments and pilot trials:

All pilot trials (data collection in specific universities in Europe, Latin America, and Asia) will be approved by local ethics committees. This means that a local ethics committee will be asked to approve the experiment protocol. Furthermore, a local data protection officer (DPO) will view the questionnaire and be asked to approve data processing. If there is no designated DPO in a local university site (outside of Europe), another qualified person designated by the local institution will be asked to check data processing.[6]

Informed consent of the data subjects for pilot trials:

In compliance with the GDPR and ethical requirements for social sciences research (cf. “Code of Ethics” of the American Sociological Association, 2018 https://www.asanet.org/sites/default/files/asa_code_of_ethics-june2018.pdf), WeNet will ask for the explicit consent of the data subjects to collect their data. Students (= data subjects in this projects) will receive information about the WeNet project and its context, the data collection process, and the purpose of the data collection process. This purpose will be defined as “research,” specified further to include machine learning and social sciences research, and principles and guidelines on the performance of this research will be provided. Moreover, the data subject will learn from the informed consent form that there are several partners involved in the project and that data gathered will be shared only in an anonymized form with one or more partners in the project. Person-related information of the data subjects will only be kept during the data collection process. Research and analysis will be conducted only with anonymized data.

Note on purpose limitation and data collection process:

Since the purpose of the data collection in WeNet is “research” or rather specific areas of research such as “scientific and statistical research,” “machine learning,” and “social sciences research,” the analysis and use of the data serves a wide range of purposes. In the informed consent form, as far as we understand in WeNet, we do not have to lay out the individual analyses that we plan to run with the data. The scope of the research purpose is broad enough to allow for different analyses. This is supported in the text of the GDPR (recital, 33):

[6] For the copies of approvals by ethics committees of the informed consent forms and of the information sheets: See WeNet Deliverable 11.1. For the technical and organizational measures that will be implemented to safeguard the rights of the participants and the data transfer from EU to Non-EU countries and vice versa: See D 11.2. For WeNets privacy operational procedure see WeNet’s internal document “Ethics and Privacy operational procedures. Cf. also “WeNet code of ethics“.

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

"It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

Some ethical concerns may arise from this and should be addressed in the WeNet consortium. For instance, data subjects may not understand the scope of possible research that they are providing their data for. Students may not be able to imagine the various scientific exercises conducted with their data and thus not anticipate possible risks arising from this. There is thus a danger of a lack of transparency deriving from the purpose "research" in the informed consent form. It may also be more difficult for the local ethics committees and DPOs to anticipate potential consequences. In this regard, WeNet will discuss open questions and specific solutions in the WeNet Data Protection Forum (more information see 4.1.2). Findings will be documented after the field trials.

Data Protection Impact Assessment (DPIA) for pilot trials:

This step is a mandatory procedure that local data controllers have to go through. The data controllers and WeNet partners at the local university site collecting and controlling the person-related data of data subjects will identify possible risks beforehand. The data controller may consult with the local DPO or designated person in charge of data protection at the local site. This procedure is to be conducted at university sites within the European Union and outside of the European Union (in Mexico, Paraguay, China, Mongolia, India). Even though countries outside of the European Union are not bound by the GDPR, the same procedures under the GDPR apply to the local "foreign" sites for the purpose of the WeNet project.

User Profile in the Envisioned WeNet Platform:

In the WeNet technology, users will be able to choose which parts of their profile will be public. That means that users control the information that is provided about themselves to the WeNet community. The only requirement for signing up for the technology is to provide an email and a name to create an account. This registration process will be verified by an authority to ensure the integrity of the digital identity (i.e. no bots allowed). While the user will then have control over who has access to their information in the WeNet community, the data produced by the user can nevertheless be seen and potentially abused by the platform operator. Therefore, restrictions of usage of user's data should be included in the guidelines or licenses for platform operators and app owners (see next section).

Use of reliable and trustworthy technology providers:

WeNet will use cloud services that provides highest security standards for the storage of data. The main cloud server will be located within the European Union. Concerning the cloud storage for the pilot trials, local data controllers may decide which service provides the best possible security and will be used for the collection and storage of data. This cloud server may not necessarily be in the country of the pilot, if it is considered more suitable to have a service outside of the country, e.g. when better options exist elsewhere.

Data preparation/data processing – pseudonymization/anonymization of the person-related data:

After completing the data collection process, the data controllers in the local sites call on the data processor to prepare and process the data. The data preparation and processing will be

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

(as it stands Nov 2019) conducted by the University of Trento. University of Trento will be the data processor and will perform the data preparation activities.

4.2. WENET DATA PROTECTION FORUM

WeNet has launched a Data Protection Forum (https://www.internetofus.eu/2019/10/22/a-world-cafe-on-data-protection/). The Data Protection Forum gives WeNet researchers a platform for intensive and substantive exchange on questions of privacy and data protection. The Privacy Forum consists of an online tool (https://elearning.internetofus.eu/), a series of mediated face to face meetings and workshops.
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 on 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.
The series of face to face meetings employs various conversational methods from business consulting as well as methods from civic education, civic involvement, civic participation and workshops with experts on persistent problems.

The goals of the forum are to:

- ➔ identify problems early
- ➔ give mutual advice
- ➔ homogenize problem-solving in WeNet
- ➔ document process
- ➔ develop new concepts and methods for integrated interdisciplinary research

The results of the WeNet Data Protection Forum are made available to the public and provide orientation for related research projects and applications.

The following issues have arisen in our research and should be addressed in the next years.

WeNet Research "Mission Statement" and Transparency about Research:

Beyond providing data subjects with information about the WeNet project, it may be helpful to release a "mission statement" with regard to research in the WeNet project. The concrete analyses that will be conducted using the data cannot be specified beforehand. Therefore, the purpose of the WeNet project is broad with only areas of research specified (machine learning, scientific and statistical research, social sciences research). It is in the nature of research that analyses depend on preliminary findings and the direction of research may be adjusted upon unexpected or interesting discoveries. Research is flexible, dynamic, and often a creative process. For this reason, while we cannot specify the concrete analyses that will be conducted, we can define the principles of research that WeNet partners adhere to.

Notion of data ownership and empowerment of user:

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

While the GDPR empowers and protects the user and data subject, many existing technologies do not reflect this ideal of user control. The WeNet platform should be user-centric. It should also constitute human-centered technology. Human-centered technologies prioritize the needs and preferences of the user or operator of the technology. The WeNet platform should empower the user by technical measures and by design, provide tangible, easily accessible tools for data control that is not only inscribed in the law but realized by the features of the technology.

Sustainable use of data and data sharing for research:

One wide-open question concerns the potential re-use and redistribution of the research data and datasets created for WeNet. If WeNet decides to provide the data sets to external researchers after the end of the project, the conditions under which this is possible have to be specified After the project has ended, the data from the project may be provided to other researchers. This, however, may create new concerns of data protection and privacy, since the data subjects have not consented to the use of their data for further, unknown research purposes. Related to this question is whether the algorithms that were created in the WeNet project will be accessable for further research.

Ethical guidelines for platform operators and app owners:

The WeNet platform will be the system that integrates different apps that may be used by the students. The platform operators and the app owners thus have a responsibility for the protection of users' data. Guidelines may help clarify this responsibility and provide ethical guidance in realizing the protection of data. To prevent misuse and potential risks to users of the WeNet platform, the guidelines demarcate legitimate and legal activities by the platform operators and app owners and restrict usage of users' data. Further information should be clarified in guidelines or licenses for the operation of the platform or apps.

Some core questions can be derived from these privacy issues that should be further discussed in the Data Protection Forum:

- ➔ What technical measures and features of the platform/app can support and enhance user control of their data?
- ➔ How can WeNet empower the user (e.g. enhance privacy literacy)?
- ➔ How can WeNet promote sustainable use of data? What possible ethical and legal challenges arise from re-using and re-distributing data among researchers?
- ➔ What concepts of accountability and responsibility do we want to apply and implement? What are measures of accountability does WeNet apply if the use of the data for research purposes violates ethics principles? How does WeNet want to mitigate the trade offs between privacy and accountability with regard to potential misuse scenarios like hate speech, trolling etc.?
- ➔ What technical measures can WeNet employ to implement privacy for specific user groups to enhance non-discrimination? What would be a justified take on what groups should be granted a right to group privacy?

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

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.

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

- ➔ 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 and who has access to the data.
- ➔ 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 provides its users with a safe and secure digital environment. This is how WeNet differs from many other digital ecosystems, where users have to re-evaluate the trustworthiness individually for each application.

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

REFERENCES

1. Capurro, R. (2005): Privacy: An Intercultural Perspective. In: Ethics and Information Technology 7, pp. 37–47.
2. 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 03/12/2019.
3. Cavoukian, A. (2012): Privacy by Design and the Emerging Personal Data Ecosystem. Available online: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-pde.pdf, last checked on 03/12/2019.
4. Cavoukian, A., Taylor, S., Abrams, M.E. (2010): Privacy by Design: essential for organizational accountability and strong business practices. In: Identity in the Information Society 2 (3), pp. 405-413.
5. Davis, A. Y.; Kelley, R. D. G. (2012): The Meaning of Freedom. San Francisco: City Lights Books.
6. Ess, Ch. (2005): "Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia). In: Ethics and Information Technology 7 (1), pp. 1–6.
7. 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 03/12/2019.
8. European Union: General Data Protection Regulation 2016/679.
9. Floridi, L. (1999): Information ethics: on the philosophical foundations of computer ethics. In: Ethics and Information Technology 1 (1), pp. 37-56.
10. Floridi, L. (2006): Four challenges for a theory of informational privacy. In: Ethics and Information Technology 8 (3), pp. 109-119.
11. Floridi, Luciano et al. (2018): AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. In: Minds and Machines (28): 689-707.
12. Foucault, M. (1975): Surveiller et punir. Naissance de la prison. Paris: Gallimard.
13. Friedman, B.; Nissenbaum, H. (1996): Bias in Computer Systems. In: ACM Trans. Inf. Syst. 14 (3), pp. 330–347.
14. Habermas, J. (1990): Moral Consciousness and Communicative Action. Cambridge, Mass.: MIT Press.
15. 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 03/12/2019.
16. Heesen, J. (2012): Computer and Information Ethics. In: Ruth Chadwick (ed.). Encyclopedia of Applied Ethics. Second Edition. Volume 1. San Diego: Academic Press. pp. 538-546.
17. Heesen, J. (2016): Big Data for a Fairer Democracy? In: International Review of Information Ethics 24, pp. 15–21.
18. Hoepman JH. (2014): Privacy Design Strategies. In: Cuppens-Boulahia N., Cuppens F., Jajodia S., Abou El Kalam A., Sans T. (eds) ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology, vol 428. Springer, Berlin, Heidelberg, pp.446-459.

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

19. Levin, S. (2017): Facebook Told Advertisers it Can Identify Teens Feeling 'Insecure' and 'Worthless'. In: The Guardian, 5/1/2017. Available online at https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens, checked on 11/12/2019.
20. Nissenbaum, H. (2010): Privacy in Context. Technology, Policy and the Integrity of Social Life, Palo Alto: Stanford University Press.
21. Rawls, J. (2005): Political Liberalism. Expanded ed. New York, Chichester: Columbia University Press.
22. Rössler, B. (2001): Der Wert des Privaten. Frankfurt am Main: Suhrkamp.
23. Segrave, M.; Vitis, L. (2017): Gender, Technology and Violence. Milton: Taylor and Francis.
24. Simon, J. (2010): The entanglement of trust and knowledge on the Web. In: Ethics and Information Technology 12, pp. 343-355.
25. Susser, D.; Roessler, B.; Nissenbaum, H. F. (2018): Online Manipulation: Hidden Influences in a Digital World. In SSRN Journal. DOI: 10.2139/ssrn.3306006.
26. Torra, V.; Navarro-Arribas, G. (2016): Big Data Privacy and Anonymization. In: Anja Lehmann et al.: Privacy and Identity Management. Facing Up to Next Steps. Cham, Switzerland: Springer (IFIP advances in information and communication technology, vol. 498, pp. 15-26.
27. Trillò, T. (2018): Can The Subaltern Tweet? Reflections on Twitter as a Space of Appearance and Inequality in Accessing Visibility. In: Studies on Home and Community Science 11 (2), pp. 116–124.
28. Westin, A. F. (2015): Privacy and Freedom. New York: IG Publishing.
29. Yeung, K. (2017): 'Hypernudge': Big Data as a Mode of Regulation by Design. In: Information, Communication & Society 20 (1), pp. 118–136.

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