

Respecting the GDPR in Online Interviewed Focus Groups

 Carolina Goberna Caride 

Chair of Public, European and IT Law
Universität Passau

Abstract

Since March 2020 the Corona virus has limited personal encounters due to social distancing measures. Thus, many data collection techniques relying on face-to-face interaction, like interviews or Focus Groups (FG), are now being practised in online environments. Such change requires the implementation of innovative measures to comply with Regulation EU 2016/679 (GDPR) and obey national data protection laws. Processing personal data of voluntary participants has to have a lawful ground and a clear purpose behind it. Moreover, the researcher has to respect legal requirements and principles for processing personal data, provide the participants with information about the research procedure and apply security measures to avoid risks to the rights and freedoms of individuals. This process has to apply to any interaction mediated by Web-Conferencing Systems (WCS). The purpose of this paper is to describe the legal requirements for conducting online interviews or FG under social distancing conditions. The project of reference for the application of these requirements is the EU Horizon2020 HELIOS project consisting of the development of a decentralised social media platform.

Key words: data protection, GDPR, data processing, research, online interview, focus groups, WCS.

Citation: Goberna Caride, C. (2021). Respecting the GDPR in Online Interviewed Focus Groups. *Journal of Audiovisual Translation*, 4(1), 42–61. <https://doi.org/10.47476/jat.v4i2.2021.175>

Editor(s): P. Orero & D. Hernández Falagán


Received: January 15, 2021

Accepted: May 28, 2021

Published: : October 30, 2021

Acknowledgement: This special issue is related to the H2020 grant no. 825585 HELIOS A Context-aware Distributed Social Networking Framework.

Copyright: ©2021 Goberna Caride. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/). This allows for unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

 carolina.gobernacaride@uni-passau.de, <https://orcid.org/0000-0003-3314-808X>

1. Introduction

Social distancing has severely limited the possibility to carry out scientific research into innovative technology by means of face-to-face interaction. Even though this situation brings about new challenges, it also offers new opportunities, such as the possibility to adapt to the new reality using technology. Thanks to Web-Conferencing Systems (WCS) as SaaS (Software as a Service), interviews or Focus Groups (FG) can be carried out online, a context in which the protection of personal data plays an important role. FG are in-person meetings conducted by an experienced chairperson or researcher, where people are invited to exchange their opinions on specific topics. The legislation to rely upon in a European context is the General Data Protection Regulation (EU) 2016/679 of 27 April 2016 (GDPR), repealing Directive 95/46/EC.

The present paper presents the legal requirements which make processing personal data lawful. First, the notion of personal data is defined and the legal grounds for processing them in research projects are introduced. The study pays special attention to online interviews in FG during test phases with participants in research projects. Furthermore, principles which play a major role in scientific research, such as the principle of data minimisation, the principle of transparency or confidentiality, are also discussed. Overall, performing online interviews by means of WCS like Zoom or Microsoft Teams has obvious benefits for users and researchers, although there are controversial points which require special attention.

The steps described below are part of the EU Horizon2020 Helios project which aim is to design and provide a decentralised social media platform to improve Peer-to-Peer (P2P) communication between users based on “trust by design,” enhancing meaningful relationships. Face-to-face interviews were planned in order to investigate the participants’ experience with the technology under development. Due to the Covid-19 crisis the task was redesigned so as to rely on online instead of in-person communication. For this reason, acquiring feedback from individuals online requires legal steps to protect personal data which are addressed below.

This paper can be applied to a variety of online interactions for research purposes in audiovisual translation. In that sense it builds on Orero et al. (2018) existing recommendations, adding information about data collection and data processing.

2. Lawful Grounds for Processing Personal Data With Scientific Research Purposes

The protection of personal data is a fundamental right set in Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU). The GDPR develops the protection of personal data of humans in the light of their interaction, wholly or partly by automated means, with public authorities or services offered by private companies, but not in the course of a purely personal activity (Article 2 GDPR). In order to process personal data, one must first understand what personal data are and under which grounds

they can be lawfully processed. This is particularly important when planning research with vulnerable people, such as children or people with disabilities, as part of data collection in experimental research on media accessibility (Agulló et al., 2018).

2.1. The Concept of Personal Data Under the GDPR

According to the GDPR personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is someone 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).

The protection of personal data applies to data processed by automated means. Manual processing is only included if personal data are contained in or intended to form part of a filing system structured under specific criteria (Recital 15 GDPR). “Automated means” refers to data processed by means of computers and software, including personal computers, laptops, smartphones, routers, e-readers, portable storage devices, cloud services, digital photos or video cameras, and any other device or application using integrated circuits or microchips (Zwenne et al., 2018). Thus, automated processing occurs when automatic devices or systems, which collect and store data following a structured organised process by specific criteria, manage the data independently of that collection taking place in a central or decentralised manner (Ehmann & Selmayr, 2018).

Not all personal data are given the same consideration. The GDPR refers to “special categories of personal data” as particularly sensitive data. The context of their processing could create significant risks to the fundamental rights and freedoms of data subjects (Recital 51 GDPR). This type of data merit specific protection and for this reason, they are considered sensitive data. Processing sensitive data is prohibited unless one of the specific cases set out in Article 9 (2) GDPR applies, e.g., explicit consent of the data subject. Sensitive data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation (Article 9.1 GDPR). Biometric data are defined in Article 4 (14) GDPR as personal data related to the physical, physiological or behavioural characteristics of a person uniquely identifying her or him.

Personal interviews are a good example with regard to the processing of biometric data. Interviews for research purposes are very often recorded, which entails documenting either the voice of the person interviewed, the image, or both. Thus, the voices of participants are precisely biometrical data which can identify an individual uniquely and therefore, imply processing sensitive data (Zwenne et al., 2018). It is, however, a subject of debate if recording alone implies processing sensitive data or

the intention of evaluating sensitive criteria predominates, for instance by processing photographs through specific technical means allowing unique identification (Recital 51 GDPR).

When personal data are processed by a natural person in the course of a personal or household activity, with no connection to a professional or commercial activity, the Regulation does not apply. This means on the one hand “activities which are carried out in the course of private or family life of individuals” (ECJ C-101/01, Lindqvist, 2003; ECJ C-212/13, Rynes, 2014) and on the other hand, personal activities which could include correspondence, the holding of addresses, social networking and/or online activities undertaken within the context of such activities. The processing of data of legal persons is not covered by the GDPR either (Recital 14 GDPR).

It may as well happen that processing data does not require identification of a data subject because identification is not necessary or no longer required (Article 11 GDPR). For example, once the researcher has acquired the necessary data from the FG, the identification of individuals may not be necessary anymore. Identification includes the digital identification of a user through authentication mechanisms such as logging in to online services provided by the controller (Recital 57 GDPR). Additionally, once processed data are anonymized, they are not covered by the GDPR anymore, as the data subject would no longer be identifiable (Recital 26 GDPR). An interesting case for future GDPR analysis, regarding anonymisation which identifies a data subject, is that of people who require the accessibility service of sign language interpretation in online interviews or conferences (Isard, 2020).

2.2. Data Controller, Data Processor and Joint Controller

An actor of reference is required in order to develop the procedures of personal data processing and to respond to requests. The GDPR establishes three actors for the possible allocation of responsibility: the data controller, the data processor and the joint controllers.

A data controller is the person who establishes the purpose and means of personal data processing and who must prove and ensure compliance with the principles of processing (Article 5.1, Article 24 GDPR), e.g., a researcher conducting an interview in a FG who afterwards utilizes the data acquired for research purposes, or a programmer or software developer. On the other hand, a data processor is a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller (Article 4.8 GDPR). The third figure is the joint controller, which refers to two or more controllers who jointly determine the purpose and means of processing. This means that they decide together to process data for a shared purpose. By means of an arrangement between each other they must, in a transparent manner, determine their respective responsibilities and their respective duties to provide the information referred to in Articles 13 and 14 GDPR. Joint controllers are jointly liable for the fulfilment of obligations. It must be borne in mind that joint liability does not imply equal liability of the entity, body, administrator or operator involved in the processing of personal data, as operators may be involved in different stages and to different degrees of the data

processing. To this end, the liability has to be assessed based on the circumstances of the particular case (ECJ C-210/16, Wirtschaftsakademie Schleswig-Holstein, 2018).

There is controversy regarding the allocation of responsibility between a researcher and the software used to collect data. In online interviews a new actor appears next to the researcher or interviewer: a videoconferencing tool connected to a server. The tool acts as an intermediary between researcher and participant. In the case of developing online interviews, the scientist would set the purpose for processing personal data and utilize WCS as means for collecting the data. Thus, there are two scenarios where personal data are processed. As will be seen in Section 5, both researcher and software developer, act as data controllers. The WCS does not process data on behalf of the controller nor does it determine together with the researcher the purpose or means of processing, nor would it share liability for the fulfilment of the researcher's purpose. As can be expected, the allocation of responsibilities regarding the processing of personal data while performing online interviews or FG may raise legal challenges.

2.3. Lawful Grounds for Processing Personal Data

Personal data processing requires a legal basis (Article 5.1.a, Article 6 GDPR), otherwise it would be prohibited and unlawful. "Processing" means any operation or set of operations 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 (Article 4.2 GDPR). It must be observed that each single step of processing needs its own legal basis, e.g., collection, recording and storage are three steps which need to be covered by a legal basis.

The possible legal bases are set out in Article 6 GDPR and, for special categories of personal data, in Article 9 (2) GDPR. As can be observed from the wording of Article 6 GDPR, more than one legal basis may be applicable to the same processing. In this case, and regarding the Helios project, "consent" and "legitimate interest" are the most suitable lawful grounds for processing personal data, also appropriate for any researcher performing online interviews or FG.

2.3.1. Consent

Processing personal data under consent as a lawful ground is established in Article 6 (1) (a) GDPR. Consent refers to the action of making a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to her or him, e.g. by a written or oral statement (Article 4.11 GDPR), including electronic means. The performance of a contract is mentioned here as according to Article 9 of the E-Commerce Directive 2000/31/EC an agreement can be concluded electronically. Electronic means are deemed

relevant where consent concludes an electronic contract, with similar legal effects as written paper contracts (Lodder & Lodder, 2018 as cited in Gijrath et al., 2018). When processing personal data is not necessary for the fulfilment of the contract it may be more appropriate to rely on the legal basis of consent, rather than on the performance of a contract (European Data Protection Board Guidelines 2/2019, para. 17–20 [EDPB], 2019).

Consent as lawful ground for processing personal data must cover all processing activities carried out for the same specific purpose or purposes. In research it is often not possible to fully identify the purpose of personal data processing at the time of data collection. In principle, research projects may tackle personal data provided that the purpose is well described. More information about this point is addressed in Section 2.4. During the development of Helios, consent is requested to comply with ethical and legal standards, such as the Helsinki Declaration from 1964 and the GDPR requirements. According to the Declaration, participants' consent is required to process their data and record the answers given to formulated questions guaranteeing privacy, anonymity and confidentiality (Sibinga, 2018, p. 59–79; Williams et al., 2017, p. 44–47).

Consent provided through electronic means requires an action from the user. Thus, silence, pre-ticked boxes or inactivity do not constitute consent (Article 29 Data Protection Working Party, Guidelines on Consent [A29WP], 2018, p. 16). Consent can be as well explicitly provided in a written and signed statement, or by filling in an electronic form, for instance by sending an e-mail, scanning a document which includes the signature, using the electronic signature or pressing a telephone button. Moreover, consent may include additional practices, such as ticking a box in an e-mail and returning it to the researcher, a browse wrap linked to the agreement located at the researcher's institutional webpage (Salmons, 2017, p. 122), or visiting an internet website, which clearly indicates the data subject's acceptance of the proposed processing of her or his personal data before the processing starts. In this regard, Salmons (2017) mentions how the provision of information concerning online research (social media research) can be achieved by multiple formats, such as hearing, viewing and reading consent and information forms (p. 123). These examples show how scientific research can comply with the legal requirement of consent for online interviews. It also shows how WCS can acquire permission from a user to process personal data without any major problem. When consent is given following GDPR requirements, the researcher (or private company) can consider that the purposes of processing data are understood, reflecting an informed voluntary decision to participate (Salmons, 2017, p. 113). Consent can be provided and as well withdrawn by the data subject in specific cases (Article 17 GDPR), the aim of which is to reflect the control of the user.

The assessment of consent, especially regarding voluntary participants, can include aspects of vulnerability. For instance, if consent from children is required, it may be directly acquired from a child above sixteen years old. Otherwise, according to Article 8 GDPR, parental responsibility over the child applies (Article 8.1 GDPR), unless a national law provides a lower limit, which cannot be below the age of thirteen. If a person provides consent not having reached the age of majority, this

renders the processing unlawful (A29WP Guidelines on Consent, 2018, p. 24–25). Filling out a form stating the age can be valid evidence in low-risk cases.

2.3.2. Legitimate Interest

According to Article 6 (1) (f) GDPR processing is lawful if and to the extent that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. An exception exists where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Here the data controller can fulfil obligations by documenting legitimate interest through a balancing test which must address four requirements: (1) assessing the controller’s legitimate interest, (2) the impact on the data subject, (3) a provisional balance and (4) applying safeguards to prevent undue impact on the individual (A29WP 2014, p. 33).

This article is in general terms relevant for direct marketing purposes and prevention of fraud (Recital 47 GDPR), as well as for ensuring network and information security (Recital 49 GDPR). It is also applicable to data transfers for internal purposes in an institution, company (Recital 48 GDPR) or transfers of data acquired in FG for scientific research purposes (Recital 113 GDPR).

2.4. Processing Personal Data with Scientific Research Purposes

The GDPR foresees specific processing situations such as the one which is drafted in Article 89 GDPR and relates to processing data for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes. Article 89 does not provide a legal basis for processing personal data like Article 6. Article 89 (1) GDPR limits privileges for research, which the GDPR contains elsewhere, and Article 89 (2) and (3) enable EU and Member States legislators to provide exceptions from certain provisions of the GDPR in the area of research. In the case of the Helios project, and in this study, the focus is set on scientific research purposes.

Scientific research refers to technological development and demonstration, fundamental research, applied research and privately funded research. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular regarding the publication or otherwise disclosure of personal data in the context of scientific research purposes (Recital 159 GDPR).

The European Data Protection Board (EDPB) defines the concept as “research projects set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practices,” (EDPB, 2020, p. 151) related to data processing activities.

Before referring to the safeguards required by the article, it is interesting to mention that when personal data are processed for scientific or historical research purposes or statistical purposes,

certain individual rights set in the GDPR may be derogated (Article 89.2 GDPR). EU or national law may allow derogations if the exercise of those rights were to impair the achievement of the scientific research purpose, the derogation being necessary for the purpose accomplishment.

2.4.1. Online Testing Purposes

One of Helios' tasks is to collect participants' feedback about the use of the technologies developed as part of the project. This task, along with personal data collection, was to be fulfilled in face-to-face interaction. In this case, scientific research required human interaction. However, due to the Covid-19 Pandemic, the task has to be adapted to the current social distancing requirements. Therefore, the research will be conducted online. Thus, not only do the participants' personal data, and the collected research data have to be safeguarded, but the possible retention of data by a WCS has to be considered as well.

2.4.2. Data Processing Subjected to Appropriate Safeguards

Article 89 (1) GDPR determines that processing personal data must be subjected to appropriate safeguards protecting data subjects' rights and freedoms, ensuring technical and organisational measures and respecting data minimisation principles. For instance, implementing pseudonymisation of data is recommended and anonymisation is accepted (Wiese Svanberg, 2020, p. 1247).

Special protection is required if the data collected were to be processed by a different data controller than the original data collector. In this case, although the purpose may remain the same, the data controller may change, or there may be two controllers. Thus, the reasonable expectation on the part of the data subject as to who controls their personal data may also change (Ehmann & Selmayr, 2018, p. 228). For example, if an online interview is conducted by a specific researcher and then shared with colleagues working on the same project or institution, the data acquired have to be equally protected by every researcher involved. This is particularly relevant when experiments are replicated across different countries, as those performed for subtitling (Romero-Fresco, 2015).

Moreover, when using WCS for the interviews, the researcher has to consider the security provided by those in their terms of service or privacy policy. This way the researcher ensures technical and privacy safeguards as well as compliance with principles of data processing and users' individual rights. This consideration may represent an additional requirement for the data controller.

3. Principles of Processing Personal Data Online

The principles to follow when processing personal data are set in Article 5 GDPR, these are: (1) lawfulness, fairness and transparency, (2) purpose limitation, (3) data minimisation, (4) accuracy, (5) storage limitation, and (6) integrity and confidentiality.

Before commencing with experimental activities, a participant has to be provided with information about the research task, about the data controller and about the relevant individual rights so that the user is able to give informed consent. This aspect will be further tackled in the following section. This information may be provided in written form, as an information sheet. In the information sheet the data controller has to describe and/or apply the principles of personal data processing. The person to provide information about the research experiment or activity validated, and to acquire consent from participants, is usually the individual performing the research activity. A WCS providing its services also has to comply with the GDPR principles.

Processing personal data in online interviews for technology validation purposes must be in accordance with the six principles summarised in Table 1.

Table 1

Data Protection Principles for Processing Personal Data

GDPR Article	Purpose	Principle	Application
Art. 5 (1)(a)	Process Data	Lawfulness, Fairness, Transparency	
Art. 5 (1)(b)	Data Collection	Purpose Limitation	Specific and legitimate purpose
Art. 5 (1)(c)	Restrict Processing	Data Minimisation	Limited to what necessary to fulfil purpose
Art. 5 (1)(d)	Accuracy	Accuracy	Keep data updated/ erase data
Art. 5 (1)(e)	Data Conservation	Storage Limitation	Store for identification until purpose is fulfilled
Art. 5 (1)(f)	Security	Integrity and Confidentiality	Protection against unauthorised/unlawful processing

Source: author's own elaboration based on the GDPR.

3.1. Lawfulness, Fairness and Transparency

Briefly described, the term “lawful” refers to data being processed on legal grounds. “Fair” processing denotes acquiring consent from an individual before processing personal data. “Transparency” embraces any information and communication relating to the processing of personal data which has to be easily accessible and easy to understand in clear and plain language. For instance, consent forms need to include information about individual rights, the purpose of the processing and be clear and concise. Natural persons should be made aware of the risks, rules and safeguards related to the processing of personal data. For more information refer to Section 4 below.

3.2. Purpose Limitation

Purpose limitation refers to the specification of which data is going to be processed, clearly assessing the lawfulness of the purpose (Article 8.2 EU Charter of Fundamental Rights). This fact is related to the “storage limitation” principle. The controller is expected to ensure that the storage period of personal data is reduced to an absolute minimum and to establish time limits for erasure or for a periodic review (Recital 39 GDPR). The purpose of processing data must be specified, explicit and legitimate and not incompatible with the original purposes when the processing relates to scientific research purposes (Article 5.1.b GDPR). The purpose of processing data should be explicitly determined at the time of the data collection, e.g. in information sheets and at the beginning of the interview with a FG.

3.3. Data Minimisation

The data collected must also be adequate, relevant and limited to the necessary information required by the controller to fulfil the purpose. This follows from the necessity of and compliance with data minimisation. This principle aims at securing the data subjects’ privacy, limiting the likelihood of identification and the data controller’s or data processor’s liability by reducing the time of exposure of the personal data.

3.4. Accuracy

Accuracy refers to the requirement that the data be kept up to date, complete and, in case of inaccuracy, erased or rectified without delay (De Terwangne, 2020, p. 317).

3.5. Storage Limitation

Personal data can be stored for identification of a data subject or participant, in the case of interviews, until fulfilling the intended purpose. The data controller must ensure that the storage limits are respected. However, there are exceptions. Data may be stored in a way that permits identification of a data subject not only during the fulfilment of the purpose but also after it has been achieved, this exception is allowed when the longer storage period serves purposes of public interest, scientific or historical research, or statistical purposes. In this regard, the storage of data must be subjected to technical and organisational measures safeguarding the rights and freedoms of data subjects (De Terwangne, 2020, p. 318).

3.6. Integrity and Confidentiality

According to Article 5 (1)(f) GDPR integrity and confidentiality refer to the manner in which data are processed, expecting appropriate security against unauthorised or unlawful processing, access, accidental loss, destruction or damage. This principle also implies a security duty for controllers and processors of personal data. If there were to be a security breach, the controller would have to inform the appropriate supervisory authority and the data subject in certain cases (Recital 85, Recital 86 GDPR). Moreover, to prove compliance with security measures, a data controller, an interviewer in FG, can provide approved certification mechanisms, such as a code of conduct (Article 40, Article 42 GDPR).

When reporting findings from research projects strongly related to social media, it may happen that participants desire to stay anonymous or be rewarded for the data given and thus, not remain anonymous (Williams et. al., 2017, p. 35). Anyhow, and under appropriate security measures, the integrity and confidentiality measures have to be respected.

4. Provision and Explanation of Information

With the provision of information, the data controller explains to the data subject who manages which data and why. Beyond complying with the applicable law, researchers must bear in mind the applicability of ethical guidelines during the planned activities with humans, including providing participants with information about the research project and consent forms. Provision of information helps, on the one hand, to explain the activity or service of concern and, on the other hand, to protect the participant in case of suffering damages.

In compliance with the principle of transparency in Article 5 (1)(a) and Article 12 GDPR, data subjects have to be provided with the possibility of exercising the rights established in Articles 13 and 14 GDPR. The data subject must be able to exercise the right to: access the data processed, rectify the data, erase the data (right to be forgotten), restrict the processing, data portability, object to the

processing of personal data, or not to be subject to a decision based solely on automated processing, including profiling. These rights are to be found in Articles 15 to 22 GDPR.

When personal data are directly collected from a data subject Article 13 applies. This is the case of online interviews with FG since the information collected by researchers is provided voluntarily by participants. The data controller shall provide them with specific information, such as: (1) the identity of the controller, (2) the contact details of a Data Protection Officer (DPO), (3) the purpose of processing and the legal basis, (4) the legitimate interest, (5) the recipients of the data, and if applicable, (6) the intention to transfer data to a third party or international organisation. Salmons (2017) provides an interesting list structuring the relevant information to share with participants before and during the activity, concerning for instance the researcher's introduction, the purpose of the study or protection measures, plus additional questions for the evaluation of potential risks in online research (Salmons, 2017, p. 131). Both the researcher and the WCS company must fulfil the steps mentioned "efficiently and succinctly in order to avoid information fatigue" (A29WP Guidelines on Transparency, 2018, p. 7, para. 8), "efficiently" regarding the information provided to participants and "succinctly" regarding their privacy policies for users.

Attention shall be drawn to the sixth point of the list, namely the transfer of data. A researcher performing online interviews may share or transfer data collected to other researchers working on the same purpose. It may happen that those colleagues do not belong to the same research institution but work in the EU and thus, under the GDPR they are considered "third parties under the direct authority of the controller or processor, authorised to process personal data" (Article 4.11 GDPR). WCS, on the other hand, offer a communication service which also transfers data to company partners for corporate transactions, business purposes, or legal reasons, among others. If these partners process the data acquired, they are also considered "third parties". If the data are just disclosed to them, they are "recipients" (Article 4.9 GDPR). If they are outside the EU/EEA, transfers must be subjected to the GDPR principles and safeguards mentioned (Article 44–46 GDPR).

5. Web-Conferencing Systems for Qualitative Research Interviews

Organising FG for investigatory purposes is a common practice in qualitative research. Interviews serve to ask users individual questions which concern the topic or the use of the technology tested. In this process data are gathered from responses to construct an understanding of the user's perception and needs (Lazar et al., 2017, p. 188–189). If the research is performed online it also has to comply with the GDPR and ethical standards.

Before the Covid-19 pandemic these groups usually took place at face-to-face meetings, although utilizing videoconferencing tools or social media was not uncommon in qualitative data acquisition (Archibald et al., 2019; Thurl et al., 2017). In 2020, social distancing measures have had an impact on personal and work-related interaction, affecting the development of FG interviews for research. To overcome such a problem WCS, collaborative communication tools are used to facilitate online

meetings by means of mobile devices (Hacker et al., 2020). These tools have become an appropriate instrument to acquire participants' feedback in validation activities. Ongoing projects could shift from FG to Online Focus Groups (OFG) or "online group interviews" (Dodds & Hess, 2020).

To use a WCS, the researcher, and in some cases the participant, will need an online account to run the activity. This account implies depending on external software, or a private company, to proceed with the online interview. For this reason, the researcher herself becomes a data subject for the WCS. Hence, for her information and for the research interview carried out with participants, the researcher has to check the terms of service and privacy policy of a given WCS before beginning the experiment. This step is supposed to guarantee privacy, anonymity and confidentiality as regards the data that the program indirectly acquires. Currently, some of the most popular videoconferencing tools are: BigBlueButton, Cisco WebEx, EYON, FaceTime, Google Hangouts Meet, Jitsi Meet, GoToMeeting, Highfive Meeting, Microsoft Teams, Signal, Skype, Whereby, Zoho Meeting, or Zoom. Not all of these systems are compliant with privacy protection laws (Berlin DPO, Version 1.4, 2020), nor with the EU Web Accessibility Directive 2016/2102 regarding access to all citizens.

All examples below come from communication mediated by Zoom, given its status as a popular WCS. Although most of the companies mentioned above are not European, Zoom and other programs still have to comply with the GDPR regarding data subjects who are in the EU (Article 3.2 GDPR).

5.1. General Benefits and Detriments of WCS

Innovative technology may be the appropriate solution for unexpected situations. WCS have proven to be the adequate instrument not to replace but to channel human communication. Participants in online interviews seem to embrace the technology for testing purposes quite positively, and so do researchers. Nonetheless, both sides also find certain drawbacks.

The overall benefits of the tools mentioned pertain to the question of convenience with regard to the location of users, accessibility and cost-effectiveness (Archibald et al., 2019, p. 4). One of the WCS which has gained special prominence is Zoom. As a whole, both, participants and researchers, seem to be quite satisfied with the overall use of the program as a method for performing qualitative research interviews. There are a number of reasons for this, including the possibility of keeping rapport with the interviewer, or the fact that there is no need to set up an account or to download the program in advance. Moreover, it provides a user-friendly design considering the screen and file sharing options. Several of these features currently exist as well in Zoom's greatest competitor, Microsoft Teams, which also permits access to a meeting from the web browser without setting up an account (Tomar, 2020).

The drawbacks of videoconferencing lie in the need to acquire reliable equipment or in the quality of the technology, such as sound or video quality, as well as connection quality and stability. Other potential problems include digital illiteracy (Archibald et al., 2019; Gray et al., 2020), and the difficulties faced by people with disabilities, as many users have trouble joining sessions. Digital

illiteracy not only poses a problem concerning access to digital communication, but also in relation to comprehension of legal policies of online services, relevant for the security and protection of personal data. WCS present privacy and security vulnerabilities (Hacker et al., 2020, p. 11). In this respect, Zoom is criticised for its deficiencies concerning data protection, which nonetheless turn up in other services as well.

5.2. Legal Benefits and Detriments of WCS

As has been seen in the previous sections, there are certain legal differences regarding data protection between face-to-face and online interviews. The differences depend on the type of data processed or the data transferred, and on the allocation of responsibility or on how and where the data are stored. Several vulnerabilities of Zoom, for instance, have been vastly exposed by academics, DPO, schools (Baden-Württemberg DPO, 24 June 2020), a public research center (Rotenberg et al., 2019), and cybersecurity institutes (Instituto Nacional de Ciberseguridad [INCIBE], 2020). In the following, WCS are approached from a GDPR perspective as SaaS for researchers to use.

5.2.1. Personal Data Processed

At the beginning of this article the concept of personal data was explained. Personal data identifying a natural person in WCS does not only include the name or e-mail address of the individual, but also information about the device used, the user's location and IP address. Additionally, a WCS acquires metadata, understanding by such the participants, the time and the location of the interaction (Berlin DPO, Version 1.4, 2020). Information about the processing is provided to data subjects by companies as part of their terms of service and privacy policies on their webpages. For instance, Zoom provides in its privacy statement a reasonably comprehensible table with information about how personal data are processed and used. The processing of these data tends to be accepted by default by consenting to contractual clauses when opening an account.

Once in the videoconference room, image and voice are usually transmitted. The use of a camera recording the image of a visible user and a microphone recording the voice of a user imply collecting sensitive data. Depending on the content of the conversation other types of data e.g., sensitive data about a third party, can be shared. In this regard, Zoom provides end-to-end encryption. Nonetheless, the data controller has to consider possible risks before commencing with the processing.

5.2.2. Allocation of Responsibility

As mentioned above, a data controller is the person in charge of establishing the purpose and means for processing personal data. As soon as a researcher utilizes a WCS to obtain a service, the researcher becomes an identified natural person for the company, and thus, a data subject whose personal data

are also being processed. In this regard, a WCS is a data controller with respect to the researcher or institution using its services.

As the DPO of the German state of Schleswig-Holstein describes, different rules apply to the person organising the videoconference, on the one hand, and the participant, on the other. The organizer should take care of the technical and organisational measures, provide information about participation rules in relation to e.g. microphone muting, attention monitoring, prohibition against screenshot taking, and control document sharing e.g., by exclusively using pseudonymous presentations to protect the privacy of the participants. The person invited as a participant must choose an appropriate environment for the call, check the functionalities available and make sure that they are provided with necessary information regarding data protection (Hansen, 2020).

Regarding the confidentiality of telecommunications, the DPO of Berlin explains that

secrecy of telecommunications does not protect (...) against the provider when using video conferencing systems. It extends to the operator of the Internet connection, but not to that of the video conferencing service. This is a loophole in the law that the European legislator has recognized. It has required Member States to extend protection to “interpersonal communications services,” including public web and video conferencing systems.

The secrecy of telecommunications refers to the secrecy of the content in the light of the right to privacy of correspondence. Thus, this explanation raises concerns about the lack of protection of the content of the communication and metadata (Berlin DPO, Version 1.2, 2020), although as previously mentioned, Zoom, for example, provides end-to-end encryption.

5.2.3. Provision and Explanation of Information

To comply with the GDPR requirements and ethical procedures, researchers shall provide participants with the information included in Article 13, addressed in Section 4, and obtain consent. This may be achieved by sending the information before the due date and, again, at the beginning of the online session. This fact does not represent a benefit nor a detriment but a new way of fulfilling legal provisions, e.g., by giving consent verbally in the conference call prior to the interview. In case the online conversations were to be automatically transcribed, it is recommended that the participants’ verbal consent and the online interview should be recorded separately (Gray et al., 2020).

In Section 4 reference was made to the six items of information to be provided to a data subject. The second one of them referred to the contact details of a DPO. This was a controversial aspect for Zoom as the U.S. company lacked an EU-DPO until summer 2020, a fact which caused problems in exercising individual rights in Germany (Rudl, 2020). Furthermore, WCS may store or share personal data with companies outside the EU based on the consent acquired from the user and Standard Contractual Clauses (SCC). This practice means that personal data might be processed in countries without similar

levels of protection if no parallel agreement exists. For instance, data transfers between the EU and the U.S. were backed by the Privacy Shield framework. However, the European Court of Justice (ECJ) deemed the framework invalid in July 2020 (ECJ C-311/18, Facebook Ireland and Schrems, 16. July 2020. [Schrems II]). Regarding Zoom, scholars from the U.S. have exposed how its privacy practices included sharing data with Facebook or Google Analytics. Privacy and security problems keep being addressed and amended by the company (Nagel, 2020).

5.2.4. Data Processing Subjected to Appropriate Safeguards

In Section 2.4.2., reference was made to the application of technical and organisational measures to protect the rights and freedoms of data subjects. These measures recommend not only pseudonymising or encrypting data, but also ensuring confidentiality, among others (Article 32 GDPR). Software applications can implement these measures by design and by default (Article 25 GDPR), added to subsequent certification.

In Zoom there are security designs which deserve a positive mention. The program counts with the help of a configuration system, which permits the inclusion of user-specific authentication methods and real-time encryption of videocalls, in addition to the selection of members invited to the call and control of the session by the organizer. However, it is known that in the past year uninvited users caused “Zoom bombing” and that the app failed to encrypt personal data (Goodyear, 2019–2020). Most WCS allow cameras and microphones to be turned off individually.

At first sight, backup recordings on servers or local drives can also represent a benefit regarding the distribution of information for research purposes (Archibald et al., 2019), although virtual storage provided by academic institutions is regarded as more reliable than a private company’s cloud storage (Gray et al., 2020), considering that many of the companies mentioned have their servers outside of the EU or EEA. This is not the case with Jitsy, with servers in Germany.

Aside from risks involved in digital data processing, WCS might also have a detrimental effect on the personal environment of online users, since private homes have transformed into offices. Researchers must raise awareness in this respect among participants so that they avoid potentially harmful behaviour, such as displaying private photographs in the background. Additionally, the use of virtual backgrounds provided by videoconferencing tools might be suggested. Staying away from AI [Artificial Intelligence] digital assistant devices (e.g., Alexa or Siri) during the research task is also recommended. It is appropriate to advise the participant to select a private room or location for the interview, as well as the use of headphones to ensure privacy and confidentiality (Gray et al., 2020, p. 1298). These measures help to protect people’s private sphere.

Various national bodies, such as the Spanish National Institute for Cybersecurity (INCIBE, 2020), the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) (Landeck et al., 2020), or DPO provide recommendations to protect online videoconferences. These recommendations indicate the need to act in accordance with the GDPR

provisions, especially regarding (1) the provision of information to users, (2) end-to-end encrypted transmission, (3) storage of documents (Baden-Württemberg DPO, 2020, 17 April), (4) the use of open-source-software and (5) the use of landline telephones for conferences (if that could serve the purpose), to comply more easily with data protection measures (Berlin DPO, Version 1.2, 2020).

6. Conclusion

Every scientific research scenario has to comply with legal and ethical requirements. The provisions of the GDPR do not apply exclusively to the current pandemic situation or online interviews, but are of more general nature. It is fortunate that researchers can rely on the Regulation and on technological advances to test technological developments online. However, in contrast to face-to-face interviews, in online interviews data are processed in two ways: by the researcher performing the interview online in OFG and by the WCS when hosting the interview. Hence, more personal data are issued and collected.

Although the GDPR sets principles and requirements to process personal data to protect the data subject, putting them into practice in online communication still remains burdensome. While private companies behind the WCS are beginning to formulate their privacy policies in a more easy-to-follow and user-friendly manner, they nonetheless remain quite long and do not adhere to similar standards. Often, each function and purpose have to be evaluated separately. Videoconferencing tools prove to be a handy solution to develop research interviews. However, acquiring consent from participants, providing information forms, verifying if the WCS comes from an EU-based company and controlling privacy policies requires more steps than performing the task face-to-face. Moreover, accessibility issues are still to be considered in most platforms since subtitles are slowly being implemented by default but none of the platforms is capable of displaying a shared screen of a sign language interpreter simultaneously with a Power Point presentation.

Even if the legal steps described seem to be exhausting or confusing in the practical applicability, the enforcement of the GDPR provisions keeps being interpreted by the ECJ. For this reason, using WCS for online interviews in OFG could serve as a use case to improve the protection of personal data. In this regard, the cooperation between technical researchers, lawmakers and technology companies is as necessary as the development of innovative solutions.

References

- Agulló, B., Matamala, A., Orero, P. (2018). From disabilities to capabilities: Testing subtitles in immersive environments with end users. *HIKMA*, 17 195–220.
- Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using Zoom videoconferencing for qualitative data collection: Perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*, 18.

- Article 29 Data Protection Working Party (2018). Guidelines on consent under Regulation 2016/679. European Commission.
- Article 29 Data Protection Working Party (2014). Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission.
- Berlin DPO, Berliner Beauftragte für Datenschutz und Informationsfreiheit [Berlin Commissioner for Data Protection and Freedom of Information] (Version 1.4, 2020, July 3). Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen [Checklist for conducting video conferences during contact restrictions]. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf
- Berlin DPO, Berliner Beauftragte für Datenschutz und Informationsfreiheit [Berlin Commissioner for Data Protection and Freedom of Information] (Version 1.2, 2020, July 3). Berliner Datenschutzbeauftragte zur Durchführung von Video-konferenzen während der Kontaktbeschränkungen {Berlin Data Protection Commissioner on the implementation of videoconferencing during contact restrictions}. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf
- De Terwangne, C. (2020). Article 5 GDPR. In L. A. Bygrave, , C. Kuner, C. Docksey (Eds.). *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 309–321). Oxford University Press.
- Dodds, S., Hess, A. C. (2020). Adapting research methodology during COVID-19: Lessons for transformative service research. *Journal of Service Management*, <https://doi.org/10.1108/JOSM-05-2020-0153>
- EDPB (2019). Guidelines 2/2019 on the processing of personal data under Article 6 (1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0. European Data Protection Board.
- EDPB (2020). Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0. European Data Protection Board.
- Ehmann, E., Selmayr, M. (Eds.) (2018). *Datenschutz-Grundverordnung* (2. Auflage) [Data Protection Regulation]. C. H. Beck.
- Goodyear, M. (2019–2020). The dark side of videoconferencing: The privacy tribulations of Zoom and the fragmented state of U.S. data privacy law. *HLRe: Off the record*, 10, 76–89.
- Gray, L. M., Wong-Wylie, G., Rempel, G. R., & Cook, K. (2020). Expanding qualitative research interviewing strategies: Zoom video communications. *The Qualitative Report*, 25(5), 1292–1301.
- Hacker, J., vom Brocke, J., Handali, J., Otto, M., & Schneider, J. (2020). Virtually in this together – how web-conferencing systems enabled a new virtual togetherness during the COVID-19 crisis. *European Journal of Information Systems*, 29(5), 563-584. <https://doi.org/10.1080/0960085X.2020.1814680>
- Hansen, M. (2020). Datenschutz: Plötzlich Videokonferenz – und nun? [Data protection: video conference - what now?]. <https://www.datenschutzzentrum.de/uploads/it/ULD-Plotzlich-Videokonferenzen.pdf>
- INCIBE (2020). Vulnerabilidad descubierta en el sistema de videoconferencia Zoom [Vulnerability discovered in Zoom videoconferencing system]. <https://www.incibe.es/protege-tu-empresa/avisos-seguridad/vulnerabilidad-descubierta-el-sistema-videoconferencia-zoom>

- Isard, A. (2020, May). Approaches to the anonymisation of sign language corpora. In *Proceedings of the LREC2020 9th workshop on the representation and processing of sign languages: Sign language resources in the service of the language community, technological challenges and application perspectives* (pp. 95–100). European Language Resources Association (ELRA).
- Landeck, N., Korbach, C., & Hermes, M. et al. (2020). *Kompendium Videokonferenzsysteme: KoViKo – Version 1.0.1. [Compendium Videoconference Systems]*. Bundesamt für Sicherheit in der Informationstechnik.
- Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research methods in human-computer interaction*. Morgan Kaufmann.
- Baden-Württemberg DPO (2020, April 17). *Datenschutzfreundliche technische Möglichkeiten der Kommunikation [Privacy-friendly technical options for communication]*. <https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/>
- Baden-Württemberg DPO (2020, June 24). *Warnung des LfDI wurde gehört – Zoom bessert nach [LfDI Warning were heard – Zoom makes improvements]*. https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/06/PM-Zoom-bessert-nach_fin.pdf
- Lodder, A. R., & Lodder, N. (2018). Directive 2000/31/EC – electronic commerce directive. In Gijrath, S., van der Hof, S., Lodder, A. R., & Zwenne, G. J. (Eds.). *Concise European data protection, e-commerce and IT law* (pp. 255–324). Kluwer Law International.
- Nagel, M. (2020). *3 New ways we're combatting meeting disruptions*. Zoom Blog. <https://blog.zoom.us/new-ways-to-combat-zoom-meeting-disruptions/>
- Orero, P., Doherty, S., Kruger, J. L., Matamala, A., Pedersen, J., Perego, E., Romero-Fresco, P., Rovira-Esteva, S., Soler-Vilageliu, O., Szarkowska, A. (2018). *Conducting experimental research in audiovisual translation (AVT): A position paper. The Journal of Specialised Translation, (30), 105–126.*
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. (General Data Protection Regulation).
- Romero-Fresco, P. (2015). *The reception of subtitles for the deaf and hard of hearing in Europe*. Bern.
- Rotenberg, M., Bannan, C., Hui, J., O'Brien, L., Parker, S., Seth, S., & Wiener, J. (2019). *Complaint, request for investigation, injunction, and other relief, before the ederal Trade Commission Washington, DC*. Electronic Privacy Information Center. <https://epic.org/privacy/zoom/EPIC-FTC-Complaint-In-re-Zoom-7-19.pdf>
- Rudl, T. (2020, July 24). *Der steinige Weg zu den eigenen Daten [The rocky road to your own data]*. Netzpolitik.org, <https://netzpolitik.org/2020/dsgvo-der-steinige-weg-zu-den-eigenen-daten/>
- Salmons, J. (2017). *Getting to yes: Informed consent in qualitative social media research*. In K. Woodfield (Ed.). *The ethics of online research* (pp. 109–134). Emerald Group Publishing.
- Sibinga, C. T. (2018). *Ethical issues in qualitative data collection and management*. In C. T. Sibinga (Ed.). *Ensuring research integrity and the ethical management of data* (pp. 59–79). IGI Global.

- Tomar, A. (2020, November 19). Bringing personal features in Microsoft Teams to desktop and web – now available in preview, Microsoft. [https://www.microsoft.com/en-us/microsoft-365/blog/2020/11/19/bringing-personal-features-in-microsoft-teams-to-desktop-and-web-now-available-in-preview/?ranMID=24542&ranEAID=nOD/rLJHOac&ranSiteID=nOD_rLJHOac-emOtBm90UgDtaWNxLgOXQg&epi=nOD_rLJHOac-emOtBm90UgDtaWNxLgOXQg&irgwc=1&OCID=AID2000142_aff_7593_1243925&tduid=\(ir_g9eve1p0w9kfqze00mmfy6qmlm2xsiih6sxxa9u200\)\(7593\)\(1243925\)\(nOD_rLJHOac-emOtBm90UgDtaWNxLgOXQg\(\)\)&irclickid=g9eve1p0w9kfqze00mmfy6qmlm2xsiih6sxxa9u200](https://www.microsoft.com/en-us/microsoft-365/blog/2020/11/19/bringing-personal-features-in-microsoft-teams-to-desktop-and-web-now-available-in-preview/?ranMID=24542&ranEAID=nOD/rLJHOac&ranSiteID=nOD_rLJHOac-emOtBm90UgDtaWNxLgOXQg&epi=nOD_rLJHOac-emOtBm90UgDtaWNxLgOXQg&irgwc=1&OCID=AID2000142_aff_7593_1243925&tduid=(ir_g9eve1p0w9kfqze00mmfy6qmlm2xsiih6sxxa9u200)(7593)(1243925)(nOD_rLJHOac-emOtBm90UgDtaWNxLgOXQg())&irclickid=g9eve1p0w9kfqze00mmfy6qmlm2xsiih6sxxa9u200)
- Thrul, J., Belohlavek, A., Kaur, M., & Ramo, D. E. (2017). Conducting online focus groups on Facebook to inform health behavior change interventions: Two case studies and lessons learned. *Internet interventions*, 9, 106–111.
- Wiese Svanberg, C. (2020). Article 89 GDPR. In L. A. Bygrave, C. Kuner, C. Docksey (Eds.). *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 1240–1252). Oxford University Press.
- Williams, M. L., Burnap, P., Sloan L., Jessop, C., & Lepps, H. (2017). Users' views of ethics in social media research: Informed consent, anonymity, and harm. In K. Woodfield (Ed.). *The ethics of online research* (pp. 27–52). Emerald Group Publishing.
- Zwenne, G. J., Steenbruggen, W., de Vries, H., Kroes, Q., van der Jagt, F., van de Bunt, T., & Kreijger, P. (2018). Regulation 2016/679/EU – General Data Protection Regulation. In S. Gijrath, S. van der Hof, A. R. Lodder, & G. J. Zwenne (Eds.). *Concise European data protection, e-commerce and IT law* (pp. 19–252). Kluwer Law International.

Case law from the European Court of Justice:

- Case 101/01, Lindqvist, ECLI:EU:C:2003:596, 3 November 2003.
- Case 212/13, Rynes, ECLI:EU:C:2014:2428, 11 December 2014.
- Case 210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, 5 June 2018.
- Case 311/18, Facebook Ireland and Schrems, ECLI:EU:C:2020:559, 16 July 2020.