PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation.

DAY TO DAY ACTIVITIES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

1 Day-to-day activities

There are many day-to-day activities that take place within the framework of ICT research (conducting surveys, creating websites, organizing conferences...). Without them it would be extremely difficult to develop an activity of this type. Each of them involves multiple and complex problems related to data protection. This chapter introduces the fundamental guidelines that researchers and innovators should follow to ensure adequate compliance with the regulations in force. The recommendations developed do not intend to be exhaustive nor do they allow us to enter into each and every detail of the activities to which they refer. Those who develop them should be sure of the particularities that their own national systems may present. In case of doubt, it is always better to have the help of a DPO or legal advisor who can advise on the issue at stake.

1.1 Organizing a congress or a conference

Lorena Pérez Campillo, José A. Castillo Parrilla (UPV/EHU)

Organizing a congress or a conference is a complicated task that involves a high number of issues in terms of data protection. Most people are not willing to have their privacy vulnerated just because they accept to attend and/or participate in an event and we must be extremely respectful with their right of privacy. Violations of basic data protection principles might bring severe sanctions to organizers.

We mainly concentrate on public events since they involve many more issues than private events. As "public events" we understand events open to the public, addressed to a considerable number of people that could complicate controlling information, or events that will be announced or published after taking place. On the contrary, "private events" would allow a better control of information since (1) the events would be addressed to a small amount of people and/or (2) the organizers have asked the participants not to publish information on the event nor images of people without their permission. Public events may have a higher risk to damage privacy, so considerations on these events must be more severe. What is said on them can be applicable to private events even when private events may not need to be as strict as public events.

DOs

- Check if software providers for the event comply with the GDPR. Verify that our U.S. suppliers or intermediaries are adhering to the Privacy Shield.
- Hold the data only for the purpose they were given to you, and only as long as you need them. After the purpose is accomplished, make sure that unnecessary data are deleted.
- Provide sufficient information in adequate formats (see informed consent section).

DON'Ts

- Do not collect or store sensitive data (medical conditions, disabilities, ethnicity) if it is not necessary. Note that the penalties are much more severe for misuse or violation of this type of data.
- Do not hold data longer than strictly necessary.
- Do not organise marketing campaigns via email for those who have not requested, consented or authorized them.

Checklist

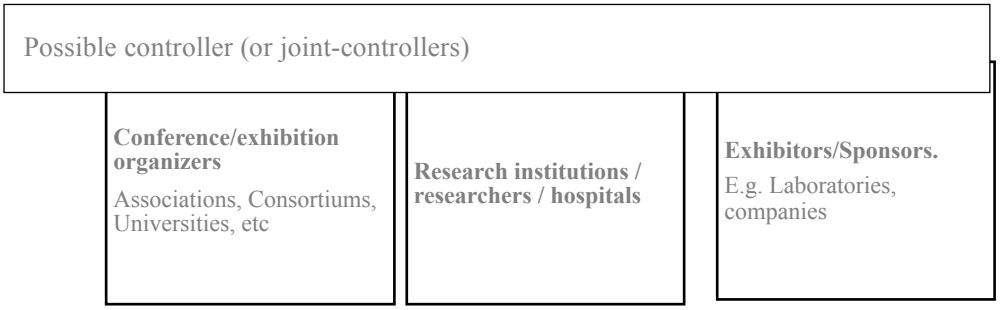
- Only personal data that is necessary have been gathered
- Personal data have not been stored any longer than strictly necessary
- Convenient measures have been implemented to ensure data subjects' rights,

interests and freedoms

- Speakers have provided consent to have their talks recorded and exhibited (if the organizer is willing to do so)

1.1.1 Some preliminary thoughts that might be particularly relevant

We assume that the research centre / group of researchers are the "controller" (see art. 4(7) GDPR) when choosing the purposes and means of the intended processing. But also, there might be *different possible controllers* as this diagram shows:



The role to be played by each organizing institution must be clarified from the very beginning of the organization process. A written agreement specifying the role to be played by each organization could be key in order to guarantee an adequate personal data processing. **If the controller works with suppliers who process data, or if there are any processors who depend on the controller**[1]**, they must make sure that processors are compliant with the GDPR and national regulation.** Examples of service providers include cloud providers or intermediary event management platforms or conferences software. It will be necessary to ensure that processors comply with the GDPR and data protection national regulations: legitimacy, duty of information, exercising of rights, etc. In addition, it will be necessary to check that the "data processing agreements" are up to date according to the GRPD. Whenever possible, controllers must **create binding agreements with suppliers to ensure that they comply both with legal requirements and with requests made by the controller (e.g. to delete or modify data).**

In a congress there are several activities that can be affected by data processing:

When organizing an event and registering attendees, we are considering general personal data (as special categories data are usually not collected), such as name, email address or provenance (e.g., entity to which they belong).

When displaying the personal data of source subjects resulting from possible scientific research, organizers might have to deal with special categories of personal data.

[1] According to article 4 GDPR, a data processor is a person, authority, agency or other body which processes personal data on behalf of the controller (art. 4.8 GDPR).

The organizers of the congress must distinguish between data that are necessary to apply for the event and other data. The requirements for consent must be different, and specify in each case (1) the purpose of data processing and (2) if providing consent for data processing is necessary (e.g., in order to allow access to the event, for any logistical or control reasons). This way, attendants can freely consent on data processing regarding data that are not necessary. Regarding data that are not necessary for the event, it must be clear that the attendants (now, data subject) can withdraw their consent at any time without prejudicial consequences (see art. 7 and WH 42 and 43 GDPR).

Apart from that, data minimization principle must be taken into account (art. 5.c GDPR). For instance, requiring email, phone number and domicile may not be necessary if the purpose of data processing is allowing contact between the organizers and the attendants. For sure, domicile would not comply with data minimization principle in this case. Depending on the circumstances, even phone number could not be necessary to contact with attendants if they are aware that email should be consulted frequently. To sum up, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

1.1.2 Some practical recommendations that might be useful

i. The purpose behind the processing of the collected data must be clear. The controller must explain whether they will use these data for publicizing future conferences, or if they will share them with the sponsors, for instance. They should provide attendees with the possibility to give separate consent to different requests. They could, for instance, use stickers to make it clear if a data subject wants to be recorded but does not want to have the recordings placed online.

ii. Management of the registration. The attendants might have different preferences about this issue. Some, for instance, might not be willing to be included in the lists of attendants. To avoid problems on the issue, a previous message should be included when collecting data (both, necessary and not necessary data as explained in point 5) warning that a list of attendants will be elaborated and distributed. This message should have the following characteristics: (1) visible: the attendants will be able to read the warning at first glance; (2) complete: the message will inform what data will figure in the list and to whom it will be distributed; and (3) reversible: the message will include a simple way to withdraw the consent warning that once the list is distributed it is impossible to recover it to withdraw data. If this list is also used to give ID cards to the attendants once arrived to the venue (if it is a physical event), the message could include a yes/no question: “would you like to receive an ID card with your name and provenance?”.

iii. Controllers must make sure about the data they really need and not ask for more. The less data they possess, the less trouble they will have. Once the event is finished, controllers must delete all data that they are not obliged to keep for legal purposes. Controllers must check the type of data that they will have to keep and the period specified by the applicable regulation. They must inform all participants about it from the very beginning.

iv. Controllers must make sure that all attendants are allowed to decide whether they want to be recorded, filmed or photographed. Gathering informed consent could be an excellent idea in this sense, but then controllers should not forget that you have to respect their right of privacy. Controllers should try to establish "camera free" zones. Some parts of the venue should be isolated from any kind of pictures or recordings. A complementary useful tool consists on preparing different cards with different colors depending on the consent/non-consent of each one of the participants to be photographed. Along with these types of measures, and once the event is held we should have some technical tool that allows to pixel or obfuscate the images in the photographs or videos, for example. We refer, for example, to recordings or photographs of a group of attendees during a lecture break.

v. If the controllers are recording the sessions and planning to include the questions and answers section, they shall advise the attendees previously. This is particularly important if panel chairs ask attendants to identify themselves before asking questions.

vi. The controllers should ask all participants (speakers, chairs…) to provide them with the biographical info and the photographs that they want to include in their short biography. Controllers must inform beforehand if people would be able to access the information. If some of them are not willing to include a photograph, controllers cannot unrespect their will. For instance, they cannot take a picture from internet and use it.

vii. If the controller needs to inform attendees or participants of some financial information to proceed with the payment of fees or to reimburse attendance costs, they shall do it from the very first communication. For example, on the corresponding form sheet. Sometimes institutions do not work well in terms of data minimization rules. The controller might have serious problems if they notice that attendees do not agree with their institutional policies on privacy and data protection issues.

viii. The controller must be aware that information about diet preferences might reveal information about religious beliefs or ideology, or even health or status (for instance, pregnancy). They must manage this information very carefully. They must try to include menus that do not result in such consequences.

1.1.3 Some tools you might use

1.1.3.1 When providing information about the processing

The controller might choose to provide basic information. If this is the case, it is advisable to include a table with the following headings so that the information can be clearly seen by the interested party:

Data Controller	*European Association XXXXC/European Society of Oncology, etc.*

Purpose of data processing	*Registration and management of event attendees*
Legitimation	*Legal obligation...*
Recipients	*No data will be passed on to third parties, unless legally obliged to do so*
Rights	*You have the right to access, rectify and delete data, as well as other rights, as explained in the additional information*
Additional information	*Additional and detailed information on Data Protection can be found on our website: www.xxxxxxx/dataprotectionpolicy*[2]

"Before filling in the form you should read the basic information on data protection presented in the link at the bottom of the table".

1.1.3.2 When taking pictures/videos of the attendees/presenters...

The controller might use a kind of information pack as the one showed below. The types of *personal data* to be collected must be indicated: how the data will be collected (e.g. photographs and videos) and where it will be collected (place). In addition, the purpose should be stated: such as marketing, training, etc. The controllers should also indicate the type of *data processing* (editing, publication, display) and whether it will be published in social media or in a newsletter.

Photography/video:

Your image and your voice can be recorded.

Please note that _____ will take pictures and video in the public areas of the conference (meeting rooms, exhibition rooms, etc.).

We may use these media in marketing materials, educational products, and publications.

They may be published in the Social Media. Tick if you agree to appear in.. Twitter Facebook LinkedIn .....

1.1.3.3 When there is streaming or photo publication...

- People should be informed, with as much information as possible, whether there will be media coverage, using identifiable external or internal media. The controller should also indicate where this will be published.

[2]All the information required in Art. 13 and 14 EU GDPR is available in the section "Data Protection Policy".

- Consent on data processing for each purpose must be different and potential data subjects must be able to clearly distinguish each one of the different consents.

Broadcast in streaming:

"We inform you that the event and during both days, will have media coverage, with external media (outside the congress, mostly national and international journalists) and internal. There are interns who have been expressly hired by _____ such as the audio-visual recording of the speakers and some interviews, for their edition and postproduction. The congress will be published online through streaming (through the following YouTube channel xxxxxxxxx).

1.1.3.4 When the events are webinars ...

- The same obligations must be fulfilled as if they were events in a physical place, i.e. there must be a legitimizing basis (consent, contractual obligation, etc.), the interested party must be informed, etc. Some requirements may need to be adapted to the digital environment.
- The corresponding research institution or researchers who organize this type of event (conferences, congresses, webinars, etc.) will include a section with the purpose "management of congresses" in which the following should be detailed:

  - Legal basis: *Contractual to formalize the registration, participation and purchase of tickets for the events.*
  - Purposes of processing: *management of attendees, registrations, management of certificates.*
  - Group of people affected: *Attendees, speakers, participants.*
  - Categories of data to be processed: *Personal data: name, surname, address, telephone, email, position, company, city and country.*
  - Categories of recipients to whom personal data may be communicated: *attendees, congress participants, researchers.*
  - International transfers: *(If there is non-European software or cloud providers with non-EU servers, there would be international transfers).*
  - Deadlines for the deletion of personal data: *(Legal deadline).*
  - Applicable safety measures: *Pseudonymization, etc.*

1.2 Creating a website

When creating a website, privacy and security should be taken into account. Both dimensions are highly connected and it is important to bear them in mind when an individual (in this case, a Researcher) or an organization (e.g. universities, private organizations, etc.) is going to create a website.

For this section, it is going to be assumed that the researcher does not have any knowledge of development, privacy, or security. Therefore, this section is going to be written attending to two different situations:

- The website is developed by a web designer; or
- Using a CMS (Content Management System, e.g. WordPress)

In both cases, privacy and security are difficult to implement when third parties are involved. For this reason, the researcher must acquire knowledge in both dimensions in order to avoid infringing data protection Laws.

The main objective of this section will be to provide enough awareness about the main topics related to privacy and security at the moment of creating a website.

1.2.1 Data protection: what to take into account at the time of creating a website

The Regulation which is going to guide this section is the 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 (hereinafter, GDPR) together with DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter, e-Privacy Directive).

e-Privacy Directive affects a website, mainly, in to aspects:

- Marketing communications: here it is important, now, to follow GDPR requirements for consent; nevertheless e-Privacy Directive has its own local Regulation. It is important to review local requirements and assess when or when not marketing communications can be sent with or without consent.
- Cookies: for this topic, please read (see section "When to set cookies and how to write your cookie policy" within Part I of these Guidelines) and follow the recommendations on how cookies have to be managed to comply with GDPR and e-Privacy Directive requirements.

Going back to the website, the process starts when the Researcher decides to create one, which represents the first milestone, namely "design phase". In line with the GDPR, we can say that this design phase is where we must ensure compliance, which is not a recommendation but an obligation of Article 25 of GDPR: Data Protection by Design and by Default.

This concept was a bit confusing when the GDPR came into force on 25th May, 2018, but Data Protection Authorities (hereinafter, DPA) have been enlightening organizations in relation to what this obligation entails.

In short, Data Protection by design and by default consists in this case in applying the necessary guarantees from an initial phase (design of the website) if personal data are going to be processed. These guarantees pervade all GDPR principles. In this case, it is the controller (when applicable, researcher/university/other organizations where the researcher works) who has the obligation to comply with this Article and ensure compliance with all GDPR principles. We have a very good example with the Spanish DPA, who has developed a guideline[3].

Each principle derives in specific measures which are going to be analyzed in this section.

1.2.1.1 Lawfulness, fairness and transparency principle

Within this principle, we can differentiate two parts: Lawfulness and fairness on the one hand, and transparency on the other.

Lawfulness and fairness:

This principle implies that personal data can be processed if at least one of the legal bases[4] identified in Article 6 of the GDPR applies. In the case of websites, normally[5], these requirements mean that it is necessary to obtain consent from the data subject.

If consent is required, the next website areas, among others, are normally the ones that require implementing an action in order to comply with the Regulation:

- **Contact section**: where the end user can contact the researcher in order to ask any question. The purpose of this processing activity is to use personal data of the end user in order to answer the question.
- **Subscribe to newsletter**: the purpose of this activity is to process personal data to send data subjects news regarding, for example, new research activities carried out during the last month.
- **Career area**: the purpose of this processing activity is to process personal data from candidates in order to perform the hiring process.

Consent requires an affirmative and positive action from the data subject (for example, clicking a checkbox accepting to share personal data with the researcher) but also requires being informed (developed later on here) and giving it freely. Freely given means that the options given to the data subject cannot be remarked, highlighted or in another way where benefits the process of these data.

As a requirement of the GDPR (Art. 7), the Researcher will need to keep a record of the consents [6]gathered on this website, but also demonstrate compliance with the other

[3] For further information, please visit https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[4] By legal basis we mean the legal justification that allows us to use personal data. Theses legal bases are the following: **consent,** the performance of a **contract**, for compliance with a **legal obligation**, to protect **vital interests**, or for the performance of a task in the **public interest** or in the exercise of **official authority vested** in the controller**;** this legal basis can be found at Article 6 of GDPR

[5] As already mentioned, other legal bases can be identified as the grounds to process personal data, which may not require the same actions as consent. Consent is the only legal basis which requires a positive and affirmative action from the data subject.

[6] Also, these consent requirements are complimented by specific guidelines from the European Data Protection Board. For further information, please visit the following link: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

requirements: informed, freely given, and unambiguous (Recital 32 together with Art. 7).

Consent must be proportional to the purpose for which the activity is carried out; it has to be specific. Giving consent to different purposes that bear no relation to one another fails to comply with GDPR requirements.

In the event that the research activity involves children, it is important to bear in mind that the GDPR establishes digital consent as the requirement for children when they are at least 16 years old (Art. 8). This Article can be modified by each Member State of the European Economic Area (hereinafter, EEA), so the Researcher must take into consideration local Data Protection Laws for this situation.

Anyway, when personal data are collected from children who are below the minimum digital age to consent to processing of personal data, parents or legal guardians must give consent on their behalf.

Transparency:

The GDPR establishes strong requirements about the information that must be given when personal data are gathered and processed. These requirements are stated in Art. 13[7] and 14 when personal data comes from public sources, which can be an important source for Researchers to obtain personal data for their activities. Nevertheless, for the case of gathering personal data through a website, Art. 13 will be the one applicable.

The common way to do this is by introducing a link to the privacy policy when consent is gathered due to the requirements already mentioned. Also, if possible, include a checkbox stating that the data subject has read the privacy policy, or ensure that the privacy policy should appear as a pop-up window when the data subject positions the mouse pointer over the consent checkbox.

Going back to the transparency principle, which is closely linked to the duty to inform, it is important for the Researcher to understand that the information must be given in a way that is easy to understand; this means that an average user must be able to clearly understand what is going to be done with their data. Using user-friendly language helps to reach this requirement, together with graphics or pictures, even videos.

In addition, information must be easily accessible for data subjects. If the information is "hidden" or the data subject has to click on several sections to reach this information, the website will not be transparent about what is being done with personal data at the time they are processed.

1.2.1.2 Purpose limitation

Purpose limitation means that personal data cannot be processed for purposes other than the ones stipulated in the privacy policy when the data were collected, unless these purposes correspond to archiving activities of public interest, purposes of scientific and historical research or statistical purposes.

[7] An example of privacy policy can be consulted within the following link: https://gdpr.eu/privacy-notice/ This is not an official source*

If the Researcher falls within the exemption of archiving activities of public interest, purposes of scientific and historical research or statistical purposes, it does not entail an exemption to comply with the transparency principle in line with the duty to inform. The Researcher must indicate in the privacy policy, if they perform these activities that the main purposes of the processing activities may change to the ones already mentioned.

Based on the different actions named in previous section 4.2.1, the following purposes can be identified:

- To answer questions from users of the website (contact section);
- To send the newsletter (subscribe newsletter); and
- To manage job positions.

These purposes will be applied to one or more processing activities. A processing activity is any operation or set of operations which is performed on personal data or on sets of personal data; therefore, we can group the aforementioned purposes in one processing activity: website management. This name is an example and the Researcher can name the processing activity as desired.

1.2.1.3 Data minimization

Data minimization requires not processing more personal data than necessary to fulfil the different purposes of the processing activity or activities identified.

As guidance to comply with the data minimization principle, three questions can be asked to help Researchers to perform a brief assessment:

- Can we fulfil the purposes already identified with fewer personal data?
- Does this reduced amount of personal data suffice to properly fulfil the purposes?
- Do we have enough personal data to properly fulfil the purposes?

By answering these questions, the Researcher will solely see if the minimization requirement is fulfilled or not; if the above questions are answered affirmatively, the Researcher must ultimately find out which personal data are strictly needed to fulfil the purposes identified.

In addition to this, the most common source where data minimization could be not fulfilled is at open fields: for example, from the contact section, anyone can send as many personal data as they want to the Researcher. This entails a risk, because these personal data will also be stored and maintained during the processing activity and once it's ended. The recommendation here is to avoid as much as possible open fields and only use closed fields to gather personal data.

1.2.1.4 Accuracy

This principle states that when personal data are collected they have to be accurate and, where necessary, kept up to date. In practice, ensuring compliance with this principle seems a difficult task.

Data quality can be preserved using technology (e.g. data analytics), requiring extensive efforts in order to achieve compliance with this principle. For this reason, the

Researcher should also bear in mind that this principle applies only when data are going to be processed (accuracy does not have to be ensured all the time), and to make this happen, there are two recommendations:

- The first one is to add a checkbox as a statement from the data subjects' side, indicating that they assure the accuracy of the personal data given. This should be mandatory for the data subjects.
- On the other hand, it would be highly advisable to include a section within the profile area on the website, giving the possibility for the data subjects to modify and update their personal data if there is any change during the activity to be developed.

These two tips will give the Researcher an easy way to comply with this principle.

1.2.1.5 Storage limitation

The storage limitation principle requires that personal data not be stored longer than needed to fulfil the purposes of the processing activities identified. In addition to this, the Researcher can store personal data longer than needed if they are processed for archiving activities of public interest, purposes of scientific and historical research or statistical purposes.

Also, different Regulations can affect the storage of personal data, such as tax obligations or criminal laws. If none of these legal obligations or other exemptions to these principles operate, the Researcher will need to define a retention period for personal data in line with the proportionality of the purposes pursued.

For the common purposes and processing activities already identified in this section (website management), the recommendation will be to not store personal data for longer periods; besides, this information should be deleted once the purpose is fulfilled. In case that personal data is used for research activities, the recommendation is to transform personal data to aggregated data (using de-identification protocols such as anonymization) where the GDPR does not apply, since aggregated data are not personal data.

Lastly, the Researcher must be aware that, if personal data are shared with third parties, they have the obligation to delete the data once the professional relationship ends. Additionally, backup policies from different solutions such as Microsoft OneDrive should be reviewed in order to ensure that data are deleted. Backups may store these data without the knowledge of the Researcher.

1.2.2 Secure the information: minimum tips to ensure information security when creating a website.

In this section, we define some cybersecurity recommendations to bear in mind at the time of creating a website.

First, it is necessary to differentiate between cybersecurity and information security, which is a common mistake. **Information Security** deals with the processes and methodologies designed to protect any information, regardless of its format. **Cybersecurity**, on the other hand, is concerned with protecting digital assets;

everything encompassing network hardware, software and information that is processed, stored within systems or transported by internetworked information environments.

About the aforementioned terms, we can say that information security is part of a broad concept of cybersecurity. In this sense, we also need to safeguard cybersecurity in order to protect all the assets involved during the processing of personal data and grant a secure environment. Nevertheless, in the world of information security and cybersecurity, we cannot affirm that we are completely safe or that the risk of materialization of a threat or event that may harm our assets is 0.

In terms of the compliance side of security, the GDPR indicates that security of processing is an obligation (Art. 32), and forces all persons and organizations to implement a high level of security in order to grant the confidentiality, integrity and availability of personal data. Integrity and confidentiality of data processing is also a GDPR principle (art. 5.1 f). However, the GDPR does not specify which measures should be implemented to grant these security dimensions further than encryption and anonymization. In fact, the controller and the processors are the ones responsible for defining these measures. Without any guidance and understanding of what is necessary to comply with the Regulation, this is a rather difficult task.

Our main goal is to offer guidance on the most important aspects to bear in mind for cybersecurity and information security, considering the most common types of attacks on websites.

The first thing to think about is providers. As already mentioned in the introduction, the most common option to create a website are:

- By means of a CMS (e.g. WordPress)
- A web designer

In both situations, we will be externalizing the service and sharing personal data with third parties. The CMS and the web designer would be a processor according to the GDPR, which entails an obligation to normalize this relationship with a contract, stipulating all the requirements set forth in Art. 28[8].

Big solution providers such as CMS have already addressed this issue. Thus, they offer their customers some solutions to comply with Article 28 requirements.

In the scenario of hiring a web designer, the Researcher may face two situations that may change the management of the contract:

- The web designer works for a company; or
- The web designer is a freelancer.

In the first case, the company may send a template to the researcher. This is because companies are used to working with other companies or customers, where processing personal data and signing a Data Processor Agreement is a common task.

[8] Following art. 28.8, the Danish Data Protection Authority has published standard clauses for the relationship between controllers and processors. It is the only Data Protection Authority that has proceeded to publish these clauses in Europe. For the Researcher's guidance, it may be useful to have this material, which can be consulted at: https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf

Then, if the company sends a template, it is important for the Researcher to carefully review the contract and see if all the requirements of the GDPR are met. To be able to do this, the best option is to compare a standard Data Processor Agreement already approved by a National Data Protection Authority (example given in the last page: Danish Data Protection Authority).

On the other hand, when hiring freelance web designers, it may be necessary to send them a template, as they are not so used to dealing directly with legal compliance. It is also important to raise the freelancer's awareness about the duties arising from the contract, in addition to those corresponding to the Researcher, in order to ensure compliance throughout the whole professional relationship.

Information Security is an important part of the contract derived from an obligation of the GDPR. To ensure the confidentiality, availability, and integrity of personal data together with the rest of the legal obligations contained in the Regulation, the Researcher must only hire and work with those processors which offer a high level of security.

To reach this goal, the common practice is to include a "Compliance Checklist" as an addendum to the contract to be fulfilled by the processor. The recommendation here is to hire those processors which fulfil the entire checklist, meaning that they offer a high level of compliance. This checklist also includes some organizational measures derived from International Standards such as ISO asking for security[9].

Also, when hiring a web designer or choosing a CMS for your website, it should not be forgotten that the Researcher entails a controller position, regarding data protection roles defined in the GDPR. The controller holds a dominant position over the processor, then, regarding processing activities of personal data, the processor must hear and follow the instructions of the controller.

1.2.2.1 Deeping into cybersecurity: CMS security tips

Once we have legally regulated the relationship between the Researcher and the processor (in this case, a CMS), we should say that these tools are not secure by default even though there are security measures in place based on the best standards in the market.

Nevertheless, there are a few tips that will improve the security of your CMS:

1. Make sure to update your CMS!

Technology is constantly changing. This has positive consequences but also negative ones in terms of cybersecurity; hackers can take advantage of old systems (as well-known as legacy systems) to discover vulnerabilities in the code which may allow a potential attack. Companies are normally aware of this, and they make updates to patch these vulnerabilities and keep the environment safe. Within your CMS management

[9] To this end, the Information Commissioner Office of the UK Data Protection Authority offers two resources: one to assess processors' compliance (https://ico.org.uk/for-organisations/data-protection-self-assessment/processors-checklist/) and another for information security (https://ico.org.uk/for-organisations/data-protection-self-assessment/information-security-checklist-report/); these two checklists can offer guidance for Researchers on what has to be sent to processors.

dashboard, you will have to regularly check out the update section and install those which improve security.

2. Passwords are one of the first steps towards cybersecurity!

It may seem to be a very basic topic, but people still use default or easy passwords (e.g. 1234/admin/password, etc.) to access the environment where their sensitive information is stored and processed. Within the FAQ section, you can learn how to build a robust password and avoid hacker attacks.

3. Roles and responsibilities: do not grant access with high privileges if not needed!

You may fall under the situation of working with a team, consisting of people who need to work in this environment and make changes or management of the web site. Make sure to manage within your control dashboard these privileges following the concept.

4. Use backups to ensure availability of information![10]

In the event of losing information, receiving an attack, or any other situation that may lead to the unavailability of the information of the website, backups are the solution to maintain this dimension untouched.

5. If you have the chance, carefully choose your host!

The best option is that your host be located in Europe. If you choose, or for any other reason it is by default located outside of the European Economic Area, you will be making international transfer of personal data, which requires taking specific measures into account (not legal and technical). You will have to make sure that your host uses a valid certificate for your website (SSL/TLS certificates, further explained in section 4.3.3).

As already mentioned, within the cybersecurity world, we cannot talk about 0 risks. All these tips to be aware of while building a CMS for the web site might be not enough to completely secure your website.

The recommendation here is to have support, if possible, from cybersecurity professionals who are always up to date regarding new vulnerabilities and security improvements, and also to have the necessary tools to improve security on your website.

If not possible, the five tips above should give a minimum of security for your website.

1.2.3 Web design: basic tips to develop a secure website

In the event that the Researcher prefers to hire a company or a freelancer specialized in web design and development, it is a common mistake to think about a web designer as a developer.

A web designer may have knowledge on development but focuses on *front-end* design. *Front-end* design refers to the work done on the website interface, not anything related to the back-end or connections to the database, etc. This is done by a back-end developer, who focuses on writing all the code that manages the relationship between the website and all systems that work to make it run.

[10] Please, for further information on storing your data properly, please read (include reference to section II.3. Storing your data within the new template)

That said, some tips can be provided to the developers during the web creation project:

- If the website allows the submission of comments or any other interaction with the user, it is important to implement captcha systems. These systems prevent a machine from acting as a user to facilitate the usage of malicious or marketing spam.
- If the Researcher includes the possibility of downloading any kind of material (e.g. brochures), it is important to use software in order to delete metadata that these documents store, because it can contain information that a hacker can use to exploit such as user names, directories, etc.
- Follow the instructions already given in the CMS section for robust passwords.
- Be able to store logs in order to facilitate them to authorities for investigation in the event of an attack.
- Back up all critical elements that allow the website to run, and do not forget the database [11]used for it. These backups must be stored in a different place from the original data, regularly verifying that these backups are made correctly. If the website is managed by a third party (which could be the situation for the Researcher), the obligation to make backups must be stipulated within the contract.
- If the Researcher is going to use a complex web environment within a project, it is important to differentiate between the pre-production environment, where tests are performed in order to verify the further changes or features that are to be implemented, and the production environment. This will make it possible to apply patches (pre-production environment) if vulnerabilities are detected, and to verify the modifications and features changed before making them visible to users.
- For the back-end developers, it is important to follow a Secure Software Development Lifecycle and Secure coding[12] routine. By using these methodologies, the Researcher will make sure to meet basic security requirements.
- Control the connections made by the website. Connections external to our website must be administered and controlled by a firewall with a proper policy configuration. This applies regardless of who manages the website (Researcher or a third party).
- If possible, perform technical audits to search for vulnerabilities. This is normally performed through a pen testing, where specialized professionals (ethical hackers) search for vulnerabilities to be corrected in order to avoid attacks.

[11] Databases are also a critical asset where personal data is stored. Therefore, is important to consider specific issued while creating a data base. Please, follow section III.3 “Creating a database” recommendations.
[12] https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf

1.2.3.1 Encryption: the importance of the SSL/TLS certificate

As already mentioned, the GDPR only refers to two security measures as a basis to ensure the integrity and confidentiality of personal data: encryption [13]and anonymization.

Encryption is a broad concept that can be applied to different assets in several ways. Focusing on website encryption, what we need to be aware of is the connection between the website and the database.

Using SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols allows ensuring security by encrypting data traffic between a web browser (e.g. Firefox) and a web server (where all the elements of the website are stored). Basically, these protocols protect the data processed within the website using two keys (public and private), making it unlikely for third parties to access data without the proper rights.

When the protocol is implemented, the website will earn the status of HTTPS (HyperText Protocol Secure) meaning that this site is protected by an SSL/TLS certification.

SSL/TLS protocols do not only transport data securely (converting plain text to ciphered text) but also act as an authentication between the receiver and the sender, allowing client-server applications to communicate in a way designed to prevent eavesdropping (interception of communication between two parties) and tampering (modifying data through unauthorized channels), among other things.

SSL/TLS encryption protocols are the most commonly used in the context of Internet connections. Nevertheless, it should be noted that SSL 2.0 and 3.0 are no longer valid due to the detection of huge vulnerabilities; it is recommended to only use TLS protocols for encryption.

DOs

- If possible, try to ask for professional advice in data protection and cybersecurity or, if the figure of DPO exists within your organization , ask for legal/security council.
- If you can't "DO" the first point, remember always to be transparent in what are you going to do with personal data, and read carefully the first sections of referred to data protection compliance.
- Choose carefully who are you going to collaborate with; if they fail in anything regarding data protection it is also going to be your fault!
- If possible, try to be updated about vulnerabilities together with other threats that might affect personal data security. Implement the necessary actions to correct them.
- If you are going to carry out a project for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, you

[13] Please read Security and Cybersecurity FAQs to understand how encryption works, the different types, and also the applications.

might fall under some exemptions regarding data protection compliance. Please read carefully this section of the guidelines to be aware on how this may affect you.

DON'Ts

- Don't carry out any activity if you are not sure about what to do regarding data protection compliance or security. It's better to take a breath and think carefully how to proceed!
- Don't gather more personal data than needed, don't store more time than needed or use tools that might compromise personal data security.
- Don't work with providers that do not offer a minimum level of security or compliance.
- Do not work with tools that have recognized vulnerabilities or where security incidents are common.
- In case of working with a web developer/designer, make sure that they follow secure coding/development standards to build, by design, a secure web environment.

Checklist

- We have assessed the necessary personal data to be gathered during our research activity, complying with data minimization principle;
- We have determined data retention periods (if applicable) to delete personal data properly, complying with the storage limitation principle;
- We have properly written all the information clauses explaining to the user all that GDPR requires to comply with transparency and fairness principle;
- We have properly assed the applicable legal basis to the processing activities of the project, complying with lawfulness principle;
- We have taken into account the recommendations regarding information security and cybersecurity to comply with confidentiality and availability principle;
- We have taken into account the fact that users can exercise their rights, setting up a specific channel for it and also a procedure to manage them properly;
- In the event consent is one of the legal basis, we have implemented the necessary measures to comply with consent requirements (informed, freely given, easy to withdraw...);
- We have read and followed all the recommendations at the phase of creating the website in terms of development or CMS usage;
- In the event of using a CMS, we have followed the basic tips recommendations to try to build a secure environment;
- We have encouraged our developers to follow SDLC standards avoiding possible bugs at code level that might enable unauthorized third party access.

1.3 When to set cookies and how to write your cookie policy

Bud P. Bruegger (ULD)

This section provides help in deciding when it is ok to set cookies and how to document your decisions in a cookie policy that informs users.

1.3.1 Objective of these recommendations on cookies

The following provides recommendations targeted at a common ICT research and innovation project. They aim at being easy to understand, simple to implement, compliant with regulations and good taste. If your needs go beyond this and your web site uses additional cookies, you need to dive in deeper (see "Further Reading" below) and take responsibility for your solution's compliance and good taste.

1.3.2 Am I really responsible for the cookies?

You might say that you just chose an existing content management system or service and have never decided to set a single cookie. So why should you be responsible?

According to the GDPR, your organization is considered to be the *controller*[14] of your web site, and is thus obliged to actually exercise control[15], and is held fully accountable[16] for what your web site does. So, it is indeed your responsibility that only permissible cookies are set. Only then are you able to provide the mandatory information[17] to web site visitors about the data you collect and about third-party recipients.

This means that if you use a service, you have to contractually oblige the service provider to support you in your obligations[18]; if you operate an existing content management system yourself, you need to find a technically skilled person to control the cookies. Even with limited technical skill, you can verify the cookies that your site sets by using a standard web browser[19].

1.3.3 Quick guide

The ground rule is to **use only cookies that are strictly necessary to supply a service requested by the user**. In more detail, this translates to the following DOs and DON'Ts:

DOs

- Set cookies only if it is unavoidable.

[14] See Art. 4(7) GDPR.
[15] See for example Art. 28(1), 28(3), and 29 GDPR.
[16] See Art. 5(2) GDPR.
[17] See Art. 14(1)(d) and (e) GDPR.
[18] See Art. 28(3) GDPR.
[19] See for example https://www.cookieyes.com/how-to-check-cookies-on-your-website-manually/ (last visited 8/5/2020).

- Set an authentication cookie to handle the login session in the (optional) restricted part of your website. Under certain conditions, no consent dialog is required for this.
- Create transparency to the user about cookies you set. (See login example below).
- Document what cookies you set in your cookie policy.
- When you write project proposals, promise only performance indicators that do not require tracking of individual web site visitors.

DON'Ts

- Avoid setting cookies on the publicly accessible part of your web site, in particular the home page.
- Avoid meaningless cookie banners and consent to set non-essential cookies on your homepage.
- Don't integrate social media with solutions that set third-party cookies without user awareness and explicit consent.
- Avoid access statistics that require unique identification of visitors (and therefore tracking cookies).
- Avoid using third-party analytics and third-party advertising.

1.3.4 Use only strictly necessary cookies

A key concept of data protection is to minimize the collected data and the impact on users to the minimum that is required by a legitimate purpose. Also, good taste tells us to avoid any unnecessary intrusion of the user. Translated to cookies, this means we want only those that are strictly necessary for the technical functioning of services that a user requests.

In most web sites of research and innovation projects, only the part for project internal communications and collaboration, i.e., the part restricted to authorized project participants, requires an authentication cookie to handle login sessions. We recommend avoiding all other kinds of cookies.

Should your web site be so special that you feel that you absolutely need other kinds of cookies, then you have to document a legitimate purpose why this is necessary and also demonstrate that no technical solution with a lesser intrusion on the user is possible. This should be reflected in the site's cookie policy.

1.3.5 But even if users consent?

Some people see user consent as a universal legal basis for setting all kinds of cookies. Unfortunately, this has even led to things such as plug-ins for content management

systems that falsely claim to achieve compliance with privacy regulations (e.g., the EU General Data Protection Regulation--GDPR). They typically use **cookie banner on the home page** stating "*We honor your privacy; click here to consent to any cookies and to continue to the content of the site*".

In Europe, according to applicable data protection law (the GDPR), this kind of consent lacks legal validity[20]. For example, the consent fails to be *informed* since users lack understanding of who tracks them, what kinds of profiles are compiled about them, and what purposes it serves. Also, the consent is not *free* since the user is not presented with a real choice, for example by an option to have reduced access when withholding consent.

Achieving legally valid consent for non-essential cookies is difficult and requires significant legal expertise. But even when successful, it is simply bad taste since it intrudes on users where it is not essential.

1.3.6 How to handle the authentication cookie

The restricted area of your site requires the use of an authentication cookie. This is strictly necessary for the service to which the user wants to log in to and therefore falls under the **consent exception**. This means that if your authentication cookie is a *session cookie*[21], a simple text next to the login button is sufficient to be compliant. The text informs that a cookie is being set when logging in.

Optionally, if you want to give users the option that the login is valid also after restarting the browser (or PC), then you need a *persistent cookie*. Since this is not strictly necessary, you now need to ask consent. This can for example be done with a check box "remember me". Make sure the default is unchecked. Again, inform the user with a text about the cookie. To keep your users informed, also state when the cookie expires and provide a link to information about how to log out.

An example for a login page following these recommendations is shown below.

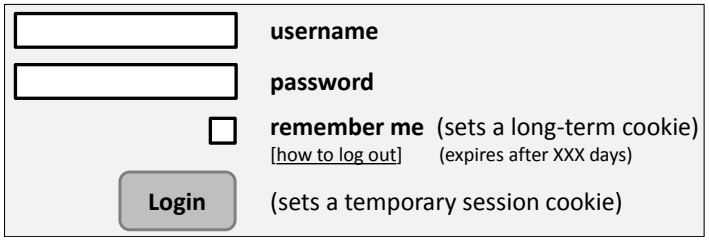


Figure 1: Example of a compliant login page.

1.3.7 Avoid third-party cookies

It is under your control and responsibility as a web site operator to decide whether to include elements (pixels, images, fonts, etc.) in your web pages that cause your users'

[20] See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf a detailed discussion.

[21] A *session cookie* is a cookie which is deleted when you close the browser. It is thus different from a *persistent cookie* which remains stored in the browser until the expiration date is reached.

browsers to fetch resources from third-party web sites. These can then set (tracking) cookies in your users' browsers.

Should you decide to involve third-party web sites in this manner, you disclose to them which of your web pages the user is visiting on your site[22]. Together with the third-party cookie that assigns a (pseudonymous) identity to your user, the third party can compile profiles of your users' behavior. Third parties, such as social media, advertisement or analytics providers, who handle users from many other sites in addition to yours, can gain insight into a large portion of your users' Internet behavior.

It is under your control to enable such third-party profiling. Also, disclosure is legally considered processing[23] for which you need a legitimate purpose and a legal basis. Since this is a legally complex area, we recommend that research and innovation project stay away and simply avoid any third-party cookies. This is also consistent with good taste that avoids exposing your users to potential privacy risks that are unnecessary for the mission of your project.

1.3.8 Careful with social media

Many projects will decide to interface their site with social media. The common plug-ins that are available for this purpose typically set third-party cookies, however. This is particularly a problem for users who refrain from having an account for the concerned social media or users who have logged out from their social media account. For these users, a third-party cookie can only be set based on consent.

But don't despair; there are data protection compliant solutions available that are valid alternatives to the common plug-ins. One example is the open source solution *Shariff*[24]. It supports all major social media and has already been integrated in a variety of content management systems including WordPress, Joomla, Type3, Drupal, MediaWiki, and several more.

1.3.9 Site access analytics

Analytics tools based on third-party cookies are very popular among web site operators. Unfortunately, they represent **a major data protection issue** and should therefore be avoided. We strongly recommend to avoid cookies for analytics altogether and base your statistics on the locally stored access log of your web server instead.

Even such access logs need some attention to be compliant: You need to limit the storage time (for example with suited configuration of your log rotation) and you should anonymize IP numbers before storage[25]. Details for how to do this are available in the "Anonymization" section of the "Main Concepts" in Part II of these Guidelines.

---

[22] Technically, this is achieved by the HTTP header "Referer".
[23] See Art 4(2) GDPR.
[24] https://github.com/heiseonline/shariff
[25] See for example, https://www.supertechcrew.com/anonymizing-logs-nginx-apache/, https://github.com/letorbi/mod_anonip (last visited 17/02/2020).

1.3.10 Cookies to support advertisements

Just say no! You are a (possibly publicly funded) research project. You don't need to create revenue by selling your web site visitor's personal data.

1.3.11 A sample cookie policy

To make the use of cookies on the site transparent, it is a good practice to offer your users a cookie policy. Here is an example that fits the above recommendations.

Cookie Policy

Overview

- We refrain from setting cookies for the public part of the site.
- We refrain from setting third-party cookies.
- We set an authentication cookie to manage your login session on the restricted part of the site. This cookie is deleted when you stop your browser. Optionally, you can choose to be remembered, in which case we set a cookie that expires after <…> days or is deleted when you log out.

What is an Authentication Cookie?

An authentication cookie is sent to your browser by the web site after you log in. It tells the browser to store a unique session identifier in your browser. The browser then sends this identifier at every access (every web page) so that the web site can recognize who you are and verify that you have indeed successfully logged in and are thus authorized to access the restricted area.

When is the Authentication Cookie set?

The authentication cookie is set on your browser after you press the login button on the login page and the web site has successfully verified your password.

When is the Session Cookie Deleted?

If you have left the "*remember me"* checkbox unchecked, the cookie will be deleted when you stop your web browser. If you checked to be remembered, the authentication cookie expires after <…> days and is then deleted. You can delete the cookie any time before its expiration by logging out. You find the logout button at the URL <…>.

Further Detail

For further information about the processing of your personal information by this web site, please consult section 8.2 of this document. The information there will also inform you about how to delete your account for the restricted area of this site.

1.3.12 Summary

Checklist

- If you don't have the necessary skills, do I have support from a technical person or my service provider?
- Do you only set cookies that are really necessary for the functioning of my website?
- Is the public part of the web site cookie-free?
- Do you always make users aware before cookies are set?
- Do you always give users the option to withhold consent to set a cookie?
- Do you always give users the option to withdraw such consent and "unset" the cookie? (See logout button above.)

1.3.13 Further reading

- Article 5.3 of Directive 2002/58/EC, as amended by Directive 2009/136/EC.
- National ratifications of the above Directive.
- Article 29 Data Protection Working Party, WP 194, 7 June 2012, Opinion 04/2012 on Cookie Consent Exemption, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf (last visited 08/03/2019).
- Article 29 Data Protection Working Party, WP 208, 2 October 2013, Working Document 02/2013 providing guidance on obtaining consent for cookies, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf (last visited 08/03/2019).

1.4 Organizing a video conference

Aliuska Duardo (UPV/EHU)

Acknowledgements: The author thankfully acknowledges the useful contributions and comments made by Manuela Battaglini and Jure Lampe in relation to this section.

Without a doubt, video-conferencing has become an essential communication tool at all levels: personal, social, business..., and, of course, its impact is also notable in the field of scientific cooperation.

This resource allows us to plan joint research and cooperation strategies, to benefit from the experience of other colleagues, thereby saving time and travel costs. Today, it is possible to prepare a research proposal at a distance, monitor the development of the project once it has been achieved, and discuss strategies and results, all via video conference.

However, from the point of view of personal data protection, there are two fundamental aspects to be taken into account when organising a video conference: the security and confidentiality of the communications; and the protection of the personal data of those involved in a video conference. In this section, we deal with the issues related personal data protection, when preparing a video conference.

DOs

- Ask your DPO for recommendations on video conferencing services.
- In case you have to choose yourself, pay close attention to the provider´s privacy policy.
- Pay attention to which Direct Personal Data is collected by the provider: You should be suspicious if more data is requested than strictly necessary to provide the service.
- Be aware of Personal Data Observed collected, and what is the purpose of such gathering.
- You should always be wary of ambiguous or empty clauses such as: "any data may be collected or disseminated, or retained indefinitely".

DON'Ts

- Mobile apps: do not install them without reading the privacy policy.
- If an app asks you to access content that is not directly related to the service they provide, do not use it.
- Do not use providers that do not identify in their Privacy Policy the types of data they collect and how they use it.
- Avoid companies that have a large number of external service providers.

Checklist

- Check if there is a specific platform designated by your institution.
- Check if your institution has any specific policies in relation to video-

conferencing tools.

- Check the privacy policy before using any tools.

1.4.1 The protection of the personal data of those involved in a video conference

Nowadays the market offers a multitude of tools and platforms that provide tailor-made video conferencing services. They can be free or pay-per-use, and allow people to share work documents and make presentations. It is also possible to choose between traditional videoconferencing that uses specific physical equipment dedicated for the purpose, and more basic systems that simply use software installed on a personal computer. There are, in addition, mobile services in the cloud, where we can hire a video conference service without having to maintain or install the classic video conference infrastructure, simply by connecting to the servers of the provider who is in the cloud. Added services, such as chat tools or virtual whiteboards, are also common.

With so many alternatives on the market, how does one choose the right tool to set up a video conferencing service that respects the privacy of the participants?

Actually, most videoconferencing service providers collect a tremendous amount of personal information in the interest of providing the service, improving the user experience, etc. In addition, all of them usually declare their commitment to respecting personal privacy, so how do you distinguish between companies that really make ethical use of personal data? Or, at least, those with which we run less risk?

Firstly, in case of doubt, it is always recommendable to seek the advice of the Data Protection Officer (DPO) of your institution - university, research centre, etc-.

In case of doubt ask to your centre´s DPO.

It is also important to choose ethical apps that respect both your privacy and that of your contacts. In order to do this, the first thing to do is to review the “Privacy policies”. A privacy policy that is too long and convoluted could be the first indication that we are dealing with a provider with non-transparent data protection practices.

A privacy policy that is too long and convoluted could be the first indication that we are dealing with a provider with non-transparent data protection practices.

In this regard, you should pay attention to which Direct Personal Data is collected by the app. Generally, these tools collect direct personal data provided voluntarily: name, email, telephone number, postal address, credit card number, etc. You should start to doubt if more data is requested than strictly necessary to provide the service. In such a case, there would be a breach of European regulation, and its main principles. Especially, the data minimization principle, whereby no more data can be collected than is strictly necessary to fulfil the purposes stated in the Privacy policy. The principle of purpose limitation will also be at stake. According to this principle, any collected data can only be used for the purpose communicated in the privacy policy; if they are used for another purpose, this must be compatible with the initial one.

What is the “strictly necessary” information? Unfortunately, it's still a lot:

Type of Information	Target	Information	Notes
User Information	Account	Valid email address or phone number.	
Transaction Information	Billing	Credit card information, billing email, banking information.	for users who choose to purchase a paid version
Transaction Information	Location	Location at the time of transaction.	Also billing address.
Metadata Information	User	IP address, geographical location,	
Metadata Information	System	Browser type and version, operating system, referral source.	
Metadata Information	Use	Length of visit, page views and website navigation paths.	As well as information about the timing, frequency and pattern of the service use.
Technical log data	Service Access	Internet Protocol (IP) address, the address of the web page visited within the Services,	
Technical log data	Access Type	Browser type and settings, information about browser configuration and plugins.	As well as language preferences and cookie data.
Technical log data	Use	The date and time the Services were used	
Device information	Device	Type of device, unique device identifiers and crash data	
Device	System	Operating system	

information		used, device settings, application IDs	

Companies usually handle more information than this we consider “strictly necessary”, but it is important that they offer at least:

- Clear links to control personal data
- An easy way to access and deletion of personal data
- Opt-out choices.

However, the most worrying thing is whether "Personal Data Observed" is collected. Here, we are talking about personal data provided involuntarily from which various types of information can be extracted.

Within this data you can find:

1. IP addresses, which provide our location.
2. Device identifiers (together with the IP address, they identify the geographical point where we are).
3. Actions performed, date and time, frequency, duration, quantity, quality, network connectivity, performance information related to logins, clicks, messages, message reading, contacts, content sharing, calls.
4. Video usage and screen sharing.
5. Messages: message content, sender and recipients, date, time and read receipts.
6. Shared content: files and file names, sizes and types.
7. Whiteboards: whiteboard content, snapshots and background images (Next).
8. Status: status information, for example, whether you are active, out of the office, or busy. In other words, with Zoom, we compromise our privacy, that of our contacts, and that of the people with whom we participate in our video conferences.
9. IP address, browser type, Internet Service Provider (ISP), referring/exit pages, files viewed on your site, such as HTML pages, graphics
10. Operating system, date and/or clickstream data for aggregate trend analysis and website and/or Product management.

At the same time, a non-transparent app frequently has a number of external service providers, and it is often unclear as to who they are, what the legal basis for data processing is, and most worryingly, if they are automatically collecting information through cookies and tracking technologies, without having asked your permission directly. In this case, not only is the legitimacy of the use of the data questionable, but there is also a risk of use incompatible with the purposes notified in the privacy policy.

You should always be wary of ambiguous or empty clauses such as: "any data may be collected or disseminated, or retained indefinitely" or "we collect your data in order to improve your user experience".

Another issue to consider, when choosing a video conferencing service, is to check the length of time our data will be stored. According to the Principle of storage limitation, this period has to be clearly specified.

1.5 Publishing/complementing data in scientific papers

Aliuska Duardo (UPV/EHU)

Acknowledgements: The author thankfully acknowledges the useful advice, and feedback on drafts from Igansi Labastida and Maria Grazia Procedda.

It is becoming increasingly common for scientific journals to require the deposition of the raw data in a public repository (subject-based or institutional) as a prerequisite for publication[26]. This practice is aimed at ensuring reproducibility, transparency and quality of research, while maximizing the benefits of sharing the results of scientific research. Such a requirement, of course, can only be demanded when data related to quantitative research is relevant to the paper. However, authors must be very careful when publishing or sharing data, so as not to affect the rights of the subjects involved in a study.

1.5.1 Legal basis for processing personal data in a scientific research

Despite the fact that the European Data Protection Regulation is not designed exclusively for research, any scientific research involving personal data must follow the GDPR rules. In this sense, article 89 recognizes the presence of a relevant "public interest" in the research which entitles the personal data to be processed, provided that appropriate measures are adopted. This entitlement implies that the legitimacy for the data processing may derive from the law, from a contractual obligation, from data subject consent, from the deployment of public interest missions, and also from legitimate interest[27]. However, GDPR imposes a very rigorous methodology involving not only European regulation but also national legislation.

1.5.2 Data sharing and informed consent

In accordance with the above, the consent of the data subject is not the only legal basis for the processing of personal data in the context of scientific research. However, the most advisable is to obtain the corresponding consent whenever possible. In any case, it is necessary to distinguish between consent for participation in research and consent to share or publish data collected.

Firstly, when working with personal data in research, it is essential to carry out a proper informed consent procedure. This ensures that the data subjects are informed and give their consent to the way their personal information will be stored or transmitted.

[26] In other cases, journals ask for the link where the data is available.
[27] Determining which basis is appropriate will depend on the research purposes and the relationship with the data subject.

However, having consent does not mean that precautions should not be taken when sharing personal information.

Whenever possible, researchers should have informed consent both for the participation in the research -always on a voluntary basis-, and for the possible uses of the information collected. Thus, the consent form should take into account any future use of the data, such as exchange, preservation and long-term use. In this regard, researchers should:

- inform participants about how the research data will be stored, preserved and used in the long term

- inform the participants about the technical measures that will be taken to ensure the confidentiality of the data

- Inform about the way of publications of results

- obtain informed consent, for the exchange/sharing of data

Without consent for data exchange, opportunities to share even publish research data may be compromised. Data from participants who do not accept publication of potentially identifiable information should be removed from the data set.

1.5.3 Preparing the data-set for publication

How to prepare data for publication in a peer reviewed journal, and avoid privacy issues?

When data is relevant to understand the scientific methodology used in a research project, peer review journals usually demand from authors a data set in a suitable format that will allow statistical analysis to be performed – namely user-friendly data. Going one step beyond the requirements by the journal, it is advisable from an ethical point of view that researchers respect the so-called FAIR data principles: research data should be 'FAIR', that is findable, accessible, interoperable and re-usable. In this sense, researchers must provide supplementary materials, and be aware of erroneous data, duplicates, or, on the contrary, missing information; they should provide sufficient information on each variable to allow other colleagues to replicate the study. Nonetheless, the publication of personal information that has been obtained, or inferred, from a research study will raise privacy issues. For this reason, the data set provided must contain the minimum level of detail necessary to reproduce all the numbers reported in the paper, while at the same time measures must be taken not to compromise the rights of the data subjects.

In this regard, Recital 156 of the GDPR points out a very valuable fact when publishing research data:

“The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymization of the data)”.

The data that allows a person to be identified can be direct or indirect. The key is the risk that people may be identified, and their privacy may be compromised, and with it other rights and freedoms, so direct identifiers must be avoided in the publication of raw data.

On the other hand, a data set with several indirect identifiers could also lead to the identification of the subject. That is why the information should be processed with a high level of security by using some or all of the following techniques: pseudonymizing or aggregating data; separating data content according to security needs; removing personal information, such as names and addresses; encrypting data containing personal information before they are stored/transmitted.

Where consent of the data subjects cannot be obtained, or there is a risk of re-identification despite anonymization measures, a careful assessment must be made on a case-by-case basis, taking into account the public interest and the scientific imperative of publication. In such cases, it is recommended that authors consult the DPO from the research Institution and relevant Ethics Committees on the legal and ethical implications of publishing their raw data in a freely accessible repository before submitting it for publication. Where the relevant committee does not exist, consultation with an appropriate national advisory body is recommended.

1.5.4 Further readings

- EDPS, Preliminary Opinion on data protection and scientific research. 1 Jun 2020. At: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (accessed March. 16, 2020)
- European Commission, Directorate-General for Research, H2020 program guidelines on FAIR data management in horizon 2020, 26 Jul 2016. At: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

DOs

- Remove direct identifiers from data sets, such as names, initials, or hospital numbers.
- Try to reduce the accuracy of detail of a variable/data through aggregation, e.g. use area rather than village, generalizing the meaning of a detailed text variable, e.g. occupational expertise; restricting upper and lower ranges of a variable to hide outliers, e.g. income, age, or by combining variables.
- If you have not been able to obtain consent and/or there is a risk of identification of the subjects involved in the research, consult the corresponding DPO and Ethics committee or equivalent national advisory body about the consequences of publishing your data.

DON'Ts

- Obtaining a general consent without specifying the exact purpose of the data processing is not acceptable.
- Alterations introduced in a data set in order to prevent identification of subjects must not distort scientific meaning.

Checklist

- Be sure you have a valid lawful basis to process/share personal data; Art. 6 GDPR.
- Pay attention to your national laws and national authorities' policies. You will probably have to meet additional conditions and safeguards set out in national law.
- Check that your research data is FAIR: findable, accessible, interoperable and re-usable.

1.6 Conducting a survey

Frédéric Tronnier (GUF)

Acknowledgements: The author thankfully acknowledges Jeanette Klonk, Andrès Chomczyk Penedo and Iñigo de Miguel Beriain

The following section provides recommendations for researchers conducting a survey in the framework of an ICT research and innovation project. They aim at being easy to understand, simple to implement, compliant with regulations, and adequate scientific practice.

In order for the survey to be legally and ethically compliant, data protection issues must be considered beforehand. Researchers should consult with their data protection officer (DPO) to receive advice on how to prepare and conduct a survey in a GDPR compliant way.

1.6.1 Planning the survey

A key principle of data protection is to minimize the collected data from respondents to the minimum that is required to achieve the specific task or purpose for which they were collected -this is called data minimization-. Researchers must always avoid any unnecessary intrusion on respondents' privacy. Therefore, researchers should think about which specific information they need for their research purpose at the planning stage of the survey. They must balance how important the data are for the project, how intrusive the questions of the survey are and whether they can collect the relevant information through less invasive methods.

According to the minimization principle, researchers should prefer anonymized data over personal data. If this is not possible (and they should be able to demonstrate why

not), pseudonymized data are the most recommendable option. Regarding the amount of data, the minimization principle forces researchers to gather as few data as possible. In this regard, opting for a large dataset must be justified. Special categories data, such as biometric data of individuals, should not be collected if this is not strictly necessary. Surveys should avoid hypersensitive questions, meaning questions that could harm respondents and/or related entities such as employers, political parties, or other individuals.

1.6.2 Preparing the survey

Before conducting the survey, researchers should address how they plan to inform potential respondents about the data protection aspects of the survey, i.e. their rights, how the processing will be done, if data will be shared with third parties, etc. In particular, researchers should carefully plan how to comply with any request from a data subject exercising one of their rights.

1.6.2.1 Obtaining respondents informed consent

Consent is a legal basis for data processing according to the GDPR. Although there are other legal bases such as the public interest (see Art. 6 GDPR), researchers should prefer respondents' informed consent to process personal data. Seeking the consent of individuals to participate in research reflects the right of those individuals to self-determination and also their fundamental right to be free from bodily interference whether physical or psychological and to protect their personal data as well as the opportunity to choose what shall or shall not happen to them. These are ethical principles recognized by human research regulation and guidelines.[28]

1.6.2.2 Online recruitment

In recent years, social media has often been used as a tool for recruiting participants in a survey. However, this practice is highly troublesome from a standpoint of data protection. To begin with, it is not easy to determine the respondent's real age. Some social media tools users involve an incredible number of minors. If a researcher recruits a minor in a survey through the use of social media tools, informed consent will not be valid (unless parental consent is provided for in compliance with the relevant national regulations). Furthermore, it might expose minors to potential risks which could harm them. Similar concerns apply to the elderly population or other vulnerable individuals, who might be unable to deal with the technologies used by the survey.

1.6.2.3 The use of tools and services

It is crucial to analyze the legality of the tools and services that are to be used for the survey beforehand. This includes services with which survey data is gathered, stored

[28] For an overview on ethics in ICT: *Ethics of information and communication technologies.* 2012. European Group on Ethics in Science and New Technologies to the European Commission. Opinion No.26. Doi: 10.2796/13541

and analyzed. Researchers must consider the following points regarding the service provider used:

- Location of the servers of the tool or service providers. Ideally, data should be stored within the EU.
- Whether data is sent to third parties.
- Availability, reliability and reputation of the service provider.
- Certification under ISO 9001/27001 or other international standards.
- Deployment of cookies to respondents.
- Whether compliance with GDPR and national legislation can be demonstrated.

In general, researchers should prefer service providers that are based in the EU and comply with European standards regarding the gathering, storing and analyzing of the survey data.

1.6.3 Compliance with national, EU and international law

The creation and execution of the survey have to comply with both European and national law. First, controllers must ensure GDPR compliance as well as any other relevant EU provision. Then, they should check compliance with national legislation as there might be specific situations referring to the research or the processing of special categories data. For instance, Art. 89(3) GDPR describes safeguards and derogations relating to processing for achieving scientific research purposes, but national regulation may add further requirements.

At an international level, most of the relevant legal documents are soft law for individuals and legal entities, i.e. not legally binding. Nevertheless, there are relevant guidelines, such as OECD "Guidelines on the protection of privacy and trans-border flow of personal data" (2013) and "Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity" (2015), which researchers should take into account. Researchers should therefore be aware of new and upcoming regulation as well as changes in existing regulation, be it national or international.

By fully understanding the legal and ethical complications of the collecting and processing of personal data in a project, controllers can ensure that the legal provisions applicable to the processing of personal data will be respected during the entire course of the project. As a general rule, all personal data should be processed in accordance with European data protection provisions, even if the data is obtained outside the EU. If your survey is conducted in an non-EU country, remember that national law may vary and make sure you comply with every national protection regulation involved as well as keeping compliance with European and international statutes on data protection. Pay special attention to any ethical rules and regulations, stemming from national laws and directives. Such national directives may require additional targeted ethical interventions.

1.6.4 After the survey has been conducted: withdrawal criteria

For a variety of reasons, a survey participant may withdraw from participating at any time after the survey was conducted. Data obtained from the respondent must be deleted immediately and not used in the results going forward. Withdrawal procedures must be compliant with EU and national law and have no consequences for the respondent. The same applies if your survey is part of a series of surveys. Therefore, the withdrawal of a participant should not only lead to the deletion of data from the last survey but also to the deletion of the data in previous surveys. You should inform survey participants about the deadline upon which they can no longer exercise their right to withdraw consent, if the data is to be aggregated and anonymized. If the data is anonymized it is no longer considered personal data and the GDPR does not apply anymore. Erasing the data from the aggregated data may then be too costly, or outright impossible. The ISO/IEC STANDARD 20889 provides an overview on privacy enhancing data de-identification terminology and techniques that may be applied to (pseudo)anonymize data. Similarly, the *right to be forgotten* is not absolute and does not apply for scientific research purposes if appropriate safeguards, according to Art.89(1) GDPR are put in place.

1.6.5 Further Reading

- European Commission: Ethics and data protection, 2018. At: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
- European University Institute: Good Data Protection Practice in Research, 2019. At: https://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/ResearchEthics/Guide-Data-Protection-Research.pdf
- ISO/IEC Standard 20889, for an overview on Privacy enhancing data de-identification terminology and techniques, 2018. At: https://www.iso.org/standard/69373.html

DOs

- Focus on personal information that is strictly necessary for the purpose of your survey.
- Carry out online recruitment carefully. Make sure that you are not recruiting minors or other vulnerable individuals or groups for your survey.
- Process and store collected data only in the way consented by the participant beforehand.
- Use explanations that are easy to understand and in a language the participant understands for the consent. Inform participants to what they give consent and what the data will be used for. Provide participants with the option to withdraw consent.
- Be aware of the ethical and legal complications of collecting and processing personal data through a survey.

- Ensure that the data is collected and processed in accordance with the GDPR even if the data is obtained outside the EU.
- Ensure that if the survey is conducted in a non-EU country, national law as well as GDPR and international statues on data protection are respected.

DON'Ts

- Don't use the data for anything other than what the survey participants consented for.
- Don't try to trick the survey participants into giving you more information than necessary.

Further Reading

- European Commission: Ethics and data protection, 2018. At: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
- European University Institute: Good Data Protection Practice in Research, 2019. At: https://www.eui.eu/Documents/ServicesAdmin/DeanOfStudies/ResearchEthics/Guide-Data-Protection-Research.pdf
- ISO/IEC Standard 20889, for an overview on Privacy enhancing data de-identification terminology and techniques, 2018. At: https://www.iso.org/standard/69373.html