UpDatAed

Toward Digitally Safe Youth Organizations

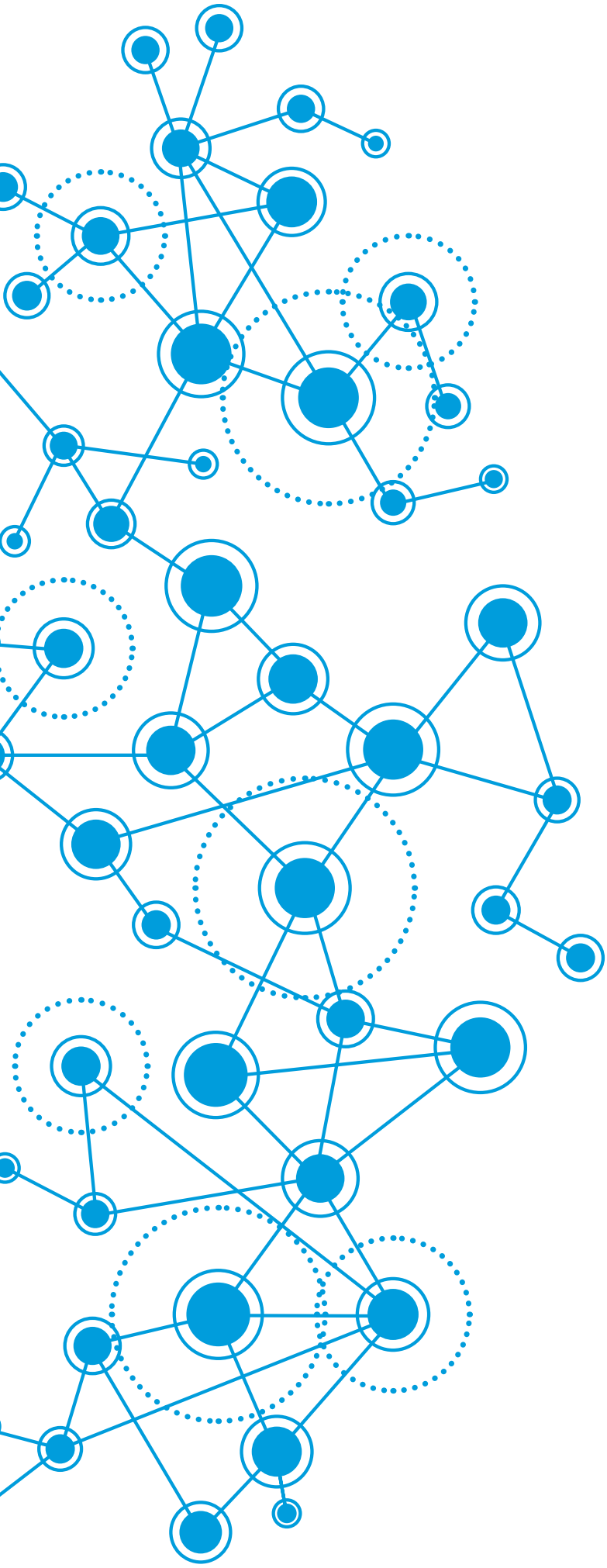
Guide for Youth Organizations on Digital Safety and Privacy

CONNECT INTERNATIONAL

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EYF

FRIEDRICH NAUMANN STIFTUNG Für die Freiheit.



Content

Introductory notes and purpose of the Guide

Youth organizations (YOs) collect and further use various types of information, including personal data. They collect personal data of their beneficiaries, members, staff members, consultants, volunteers, etc. Their work on daily basis relies on the use of such data.

The purpose of the Guide is to support YOs to improve their practices of collection and further use of personal data and to make their operation safer. Particular emphasis will be on practices in the digital environment. However, we will not neglect importance of adequate use of personal data in non-digital form.

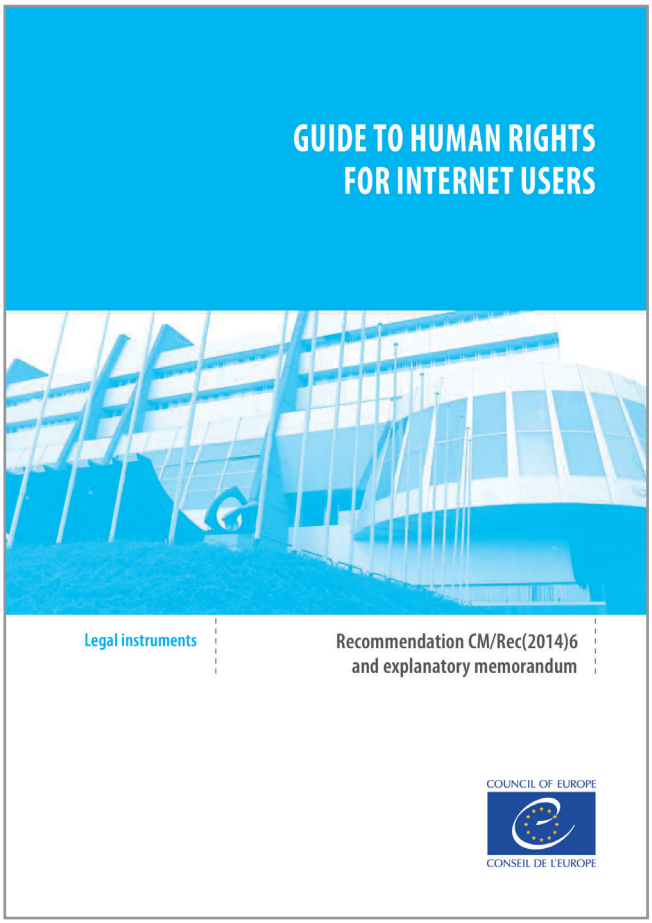
Please bear in mind that this Guide does not provide legal advice. You should not perceive it as a tool for compliance with the General Data Protection Regulation (GDPR), national data protection rules or any other binding document. For such purposes, we advise you to consult available guides on compliance with data protection legislation and find out more about applicable practice of relevant national data protection authorities.

Intersection of this Guide and the Council of Europe Guide to Human Rights for Internet Users

In 2014 Council of Europe adopted The Guide to Human Rights for Internet Users[1] "with the purpose to explain in user-friendly terms the rights and freedoms guaranteed to internet users by the European Convention on Human Rights" and to "educate individual internet users on their online rights"

Taking into account that YOs represent interests of young people and fight for their rights, we advise you to use CoE Guide for your advocacy and outreach efforts in a variety of domains, including freedom of information, anti-discrimination, education, privacy and data protection, etc.

This guide, however, addresses one particular domain of the CoE guide – privacy and data protection in the context of digital safety. Therefore, its scope is quite limited. Moreover, its approach is somewhat different. Its primary target group is not general public. Rather than that, it aims to help YOs to address their responsibilities and appropriately improve their digital safety by protecting privacy and data protection rights of the people they interact with.



[1] Available at:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680d5b31

Why is privacy so important?

What is privacy?

In this Guide we will refer to privacy as the ability of an individual to control the use of its personal data.

Why should we protect citizens' data?

The aim is not to protect data as such, but to protect citizens by restricting access to their data and by limiting activities that affect them.

Some people say – *it you have done nothing wrong, you have nothing to hide*. However, we should not confuse privacy with hiding. Privacy is a fundamental human right and therefore needs to be protected.

Moreover, privacy is a mechanism for protection of other human rights and freedoms.

For example, activists' work may be put in jeopardy if their communication is monitored. Therefore, we need privacy to exercise our freedom of expression and political association. Generally speaking, democratic regimes are the ones that respect citizens' privacy the most.

Another example – What if someone you don't trust gains access to you medical record or learns about your sexual orientation without your approval? In such cases you may become a victim of discrimination. Therefore, we protect personal data to prevent unequal treatment.

Why YOs should be pioneers in protecting citizens' privacy?

YOs promoting values of rule of law, human rights, democracy, tolerance and open society should demonstrate adherence to such values. This relates to processing of citizens' data as well. YOs should lead by example. It raises their credibility among beneficiaries and in the community. It increases trust and builds reputation. It makes them reliable in relations with citizens in need, because they will know that their personal data will be used properly.

Council of Europe Guide to Human Rights to Internet Users

Key privacy-related definitions and terminology

What is personal data?

Personal data is any information that directly or indirectly may lead to identification of an individual.

Typically, the most common type of personal data used by YOs are:

- Name
- ID numbers
- Address
- Bank account number
- Emails and phone numbers
- Level of education, etc.

However, YOs may collect and further use much more personal data. For example, you probably take photos at the events you organize. A photo may also be considered as personal data if its quality enables identification of a person.

It applies to one's IP address also, if it may help someone to identify that person.

If you provide legal support to young people, any information that relates to that individual (for example, medical data, criminal record, sexual orientation, etc) is also considered as personal data.

So, consider the definition of personal data as broad as possible.

Data processing

Data processing is basically any activity you undertake which involves personal data. So, it typically refers to collection, use, disclosure, multiplication, etc.

A common mistake is that this term applies only to physical handling of personal data. No. Even storing a file comprising of a list of participants at a meeting means that you process personal data. As with the definition of personal data, consider applying definition of data processing as generous as possible. Anything you do with personal data means that you should apply data protection rules.

Should all personal data be protected in the same way?

Generally, speaking, all personal data should be protected to avoid misuse of unlawful use. We protect data to protect people the data relate(s) to.

Some data are used more frequently. It may mean that they are accessible to more people, which may increase risks for any misuse. However, let us consider damage that may occur if certain categories of data are compromised.

For example, your mobile phone number is probably available to more people than your bank account number or your medical record. However, damage that may result from your medical record being stolen, or your bank account number being compromised, may be higher than if someone shares your mobile phone number without your approval.

There are some categories of personal data that are particularly important to protect. The types of personal data that are considered as **special categories of personal data** per the General Data Protection Regulation (GDPR) are the ones revealing:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- data concerning health of individual's sex life or sexual orientation.

If such data are compromised, significant damage may occur. Therefore, higher standards should be applied both in terms of conditions for the use of such data and for their protection.

When designing data protection measures, YOs should prioritize:

- Processes involving special categories of personal data,
- Processes with higher risk of misuse (accidental or deliberate),
- Personal data that – if compromised - may lead to discrimination of an individual or any other serious consequence.

Data controller

Data controller is.... your organization if it collects and further uses personal data. This is the term that fits you role, per data protection rules you need to apply.

However, there is another term that describes those that use personal data – data processor. It is usually a company that you contract to perform some services for you that involve use of personal data. Typically, data processor is:

- Your Cloud provider,
- A company that you contract to refund travel costs of participants at your events,
- An HR company you hire when recruiting staff members, etc.

Data processor is forbidden to use the data for any other purpose. In case you do have such arrangements with data processors, bear in mind that you are responsible for any misuse of data. To prevent that, make sure that you instruct each data processor what types of activities it needs to perform.

Data subject

Data subject is a person whose personal data you process. In this guide we will sometimes use some other terms and refer to that person simply as *person*, *individual*, *citizen*, etc. Data subject is a natural person; therefore, data protection rules do not apply to legal entities.

Typically, YOs hold information about the following types of data subjects:

- Participants at events,
- Staff members (regardless of the type of engagement per labour law regulations),
- External experts and consultants,
- Volunteers,
- Individuals to whom you provide various support (for example, legal aid, or psychological support),

Consent

For every data processing practice there should be a legal ground. Otherwise, your practices are unlawful and you are at risk of being fined.

Consent is one of such legal basis. Consent is basically a permission you obtain from the data subject, to start using its personal data. Consent needs to be:

- **Freely given**. Data subject has to have options, including to say no. Do not make taking photos mandatory at your events – your participants may oppose and they have a right not to consent to that. It should not affect their attendance at the event.
- **Informed**. All pertinent information should be provided before you start collecting personal data. Including: who are you, what do you intend to do with the data you collect, etc. Avoid complicated legal terminology and use clear and plain language.
- **Specific**. There should be no general consent for any activity you may want to undertake by using personal data. Let's assume you collect contact data of conference participants with the purpose to organize the event (to avoid delays, inform participants about change of venues, etc). Their consent relates to that activity only. If you want to further send them offers for your services, you should obtain consent for that as well, because that's not why they had registered for.
- **Unambiguous**. Avoid opt-out approach. "Silence, pre-ticked boxes or inactivity" are not allowed – says the GDPR! You may obtain consent through a statement, or an activity that clearly demonstrates that the data subject has provided consent.

General Data Protection Regulation (GDPR) in brief

When does the GDPR apply?

Well, this depends on where your YO is registered and operational, and what kind of activities it conducts.

- If your organization is registered in the European Union,

Then the GDPR applies to your YO.

Any data processing activity that you undertake falls in the scope of the GDPR and you need to comply with the GDPR anytime you collect and further use personal data. It doesn't matter if you collect data of EU citizens, residents, or residents of non-EU countries. What matters is the fact that you operate in the EU.

- If your organization is registered outside of the EU,

Then the GDPR may apply to your YO in some cases.

If your organization offers goods or services to residents of the European Union, irrespective of whether a payment is required, then the answer is YES. That typically applies to tourist agencies of airline companies. But you should check if you provide any service or goods to EU residents before you conclude that you have no GDPR responsibilities. For example, if you offer and facilitate exchange opportunities to students residing in the EU, you would need to apply GDPR rules in such operations.

You should also comply with the GDPR if you conduct monitoring of behaviour of residents of the EU, provided that their behaviour takes place within the European Union. This applies typically to internet giants, social networks and other online services. It does not apply to you if you just use social networks for targeted marketing, for example. So, your organization probably does not fall under this category. Nevertheless, you should have this requirement in mind and consider it within your process of making your organization digitally safer.

Also, bear in mind that even if you do conduct any of such data processing practices, the GDPR applies to your organization only within the boundaries of such data processing practices. So, as an organization registered outside of the EU, you may be required to comply with the GDPR when offering some services to residents of the EU. But on the other hand, your data processing activities in terms of labour relations or organization of conferences remain within the scope of your national data protection legal framework only.

Penalties under the GDPR

Penalties under the GDPR may be huge. They could significantly endanger business operation of a data controller that fails to use citizens' data adequately. So far, the highest penalty issued under the GDPR is 50 million Euros (against Google).

However, even non-monetary penalties may significantly shake up data controllers. Their reputation may be destroyed even if there is just a gossip on inadequate handling of users' data. For YOs that is an additional argument for improving their data processing activities – your beneficiaries have trust that you would use the data adequately. Don't spoil that trust.

GDPR Principles

The GDPR sets a list of data processing principles. If you apply these principles, your data processing practices will be much safer. Let us briefly explore them.

- **Lawfulness, fairness and transparency.** Make sure that you always have a legal ground to process personal data, which you should define case-by-case. Do not use personal data you obtain against best interests of the data subject. Whatever you do with personal data – keep data subjects timely informed about your practices.
- **Purpose limitation**. Make sure you use personal data within the boundaries of the purpose you want to achieve. For example, if you have obtained CVs from individuals responding to your job vacancy (including contact details), do not spam them with invitations for your seminars. They wanted to interact with you because they needed a job. Data collected for purpose A should not be used for purpose B.
- **Data minimization**. Collect the amount of data that fits the purpose of data collection. For example, if you are organizing a conference, you probably do not need information on participants' blood type.

- **Accuracy**. Make sure that personal data you store are not incorrect or misleading. Don't be afraid – that doesn't mean you need to check if participants at your prior events have changed their last names due to a new marital status. This is not a purpose of this principle. Rather than that, it aims to prevent unwanted consequences for data subjects resulting from decisions or acts based on incorrect or misleading information about them.
- **Storage Limitation**. Sometimes there are explicit rules for how long you should keep the data. Adhere to such rules. When such rules are not put in place, make sure you store data no longer than necessary. For example, you probably don't need job candidates' CVs for an unlimited or unspecified period of time.
- **Integrity and confidentiality (security)**. YOs should ensure security of personal data, by creating a work process that prevents unauthorized or unlawful access and use of personal data. A necessary prerequisite for this is to understand your data infrastructure, which we will address in the following chapter of the Guide.
- **Accountability**. This principle combines the previous ones and adds a new value – **you** are responsible for the state of implementation of data protection rules in your organization. This is not a one-time-task, but a never ending, evolving process. Develop, implement, evaluate and review your data protection internal mechanisms. Act proactively. Be ready to bear consequences in cases of incidents.

Data subject's rights

Data subjects have a variety of rights per the GPDPR. You may have heard about some of the rights, including the right to:

- Withdrawal of consent,
- Be informed about data processing practices,
- Rectification,
- Data portability,
- Be forgotten, etc.

However, we will not further elaborate these rights, as the purpose of the Guide is to support YOs to improve their practices of collection and further use of personal data and to make their operation safer. For advises on how to address legal requirements arising from specific GDPR provisions establishing data subjects' rights, assuming such provisions are applicable for operations of your YO, we advise you to further explore relevant legislation and seek for available compliance support.

In the following chapter, we will help you to map your data infrastructure. This should further enable you to:

a) recognise weaknesses and blind spots inside your existing data processing practices, and
b) develop and implement measures to improve safety of your operations.

Know Your Youth Organization's Data Infrastructure

These are the

A) tools/steps that will help you to
B) recognize internal operations and daily routines which you need to improve, in order to
C) be digitally safe and to adequately use personal data.

A → **B** → **C**

To do that, involve your team members to discuss your data processing practices.

Make sure that you encourage participants to contribute. Make sure that honesty is appreciated; even it may result in recognizing bad practices. Remember, the goal is to improve your practices. It can't be done if you are not ready to dive in and critically assess your practices.

At the very beginning, you need to understand your data infrastructure. Basically, you should know:

1. Which data have you collected so far,
2. In which data sets are the data stored,
3. How is this data set stored and where is located,
4. Who has access to each data set,
5. Which measures have you undertaken to secure each data set.

The first step is to recognize what kind of data you already have.

Discuss what kind of activities you conduct that include collection of personal data (e.g. organization of training or a conference, recruitment of new staff members, etc.).

Map all the data you collect when conducting particular activity.

IMPORTANT: While doing this exercise, you do not need to go through the data of specific individuals (e.g. Rodrigo Lopes, born in Faro, Portugal on 18 July 1995, BA in biology, bank account no 123456-789, etc). Instead, you should recognize categories of data (e.g. name, surname, place of birth, date of birth, education, bank account number, etc.)

You may have different data on the same individual within different data sets. For example, you may have your employers' data collected for labor law relations, and different data of that person collected at a training he/she attended. This is important to distinguish because different rules may apply to different data sets.

To conduct this exercise, split the data in the following manner:

- **General data (G)** – These are the data you collect so that your organization could essentially operate. E.g. data on your employees, members of the assembly or other internal bodies.
- **Programme/project data (P)**. These are the data you collect while implementing your activities, e.g. trainings, legal aid, public events, etc.
- **Other (O)**. Any other category that does not fit into G or P.

Fill in the table below. Examples are provided to help you use the table. But you should explore all data processing practices in your YO and elaborate them in the table.

1	2	3
Type of data	**Title of data set**	**Categories of data**
G	Employees	e.g. Name, surname, age, education, religion, photo, email address
P	Training participants	e.g. name, surname, email, company/ organization
P	Newsletter subscribers	...
G	Job candidates	...

The next step helps you to recognize where these data sets are located and who has access to it. Be aware that the same data set may be located in several computers within the office. It may be also available to external partners (e.g. accountant). It may be physically located in your office or in the Cloud. Finally, the same data set may be in your computer, and at your desk or in the locker, in printed form. Try answering the following questions regarding each data set.

Use the table below. Examples are presented to navigate you through the answers.

1	2	3	4	5	6	7	8	9
Type of data	**Title of data set**	**Categories of data**	**Is the data set available in digital and/ or printed form?**	**Is this data set physically located in your office only?**	**Who has access to the data set within the office?**	**If 5. NO, where is the data set located also?**	**Who also has access to data within the data set?**	**How secure is the data set?** *(Initial assessment)*
Use your inputs from the previous table	*Use your inputs from the previous table*	*Use your inputs from the previous table*	**P** - Printed, **D** - Digital, **PD** - printed and digital	**Y** - Yes, **N** - No	e.g. Project coordinator, Volunteer, Finance administrator, Director	e.g. Cloud provider, Former employee	e.g. Tax administration, Accountant	Every information is relevant. Try answering the following questions: • Do we have a system of user roles? • What is our password policy? • Do we have locked cabinets? • Do we use private emails for sharing business documentation? *Discuss any other relevant question.*
...	...	...	...	...	...	...	...	...

Once you complete this exercise, you should have improved knowledge on your data processing routines. You should also be able to implement the advices on how to improve your data processing practices, which are elaborated in the chapter ***The Steps Towards a Digitally Safe Youth Organization.***

The Steps Towards a Digitally Safe Youth Organization

This chapter will help you to examine if you use the data adequately and will provide practical guidelines how to improve digital safety of your YO.

Let us run through typical data processing practices of YOs.

1. General data and core operations

General data are the data you collect so that your organization could essentially operate. E.g. data on your employees, members of the assembly or other internal bodies. Also, here we will refer to some steps you need to undertake regardless of specific projects you implement.

1.1 Develop an Internal rulebook on data processing and data protection

This document is your *Privacy ID*. It identifies your data processing practices in the eyes of the public. It is also an important document for your staff members. It sets the rules that every staff member should apply.

For example, you may use the following language, but make sure it fits practices of YOUR organization:

The YO's internal Rulebook on Personal Data Protection

The purpose of this Rulebook is to provide legal security and transparency in terms of processing of personal data of employees, beneficiaries and other persons whose data we process. The Rulebook presents the legal basis, purpose of processing, types of data being processed, rights of data subjects with regards to personal data processing, data protection measures, etc.

The Rulebook also establishes the obligations of employees in terms of personal data protection. It applies to associates, consultants and other persons contracted by our organization.

Employees are obliged to respect and protect personal data that they process in the work occurring in the office or elsewhere. Employees can process only the data to which they are allowed access, in accordance with tasks they perform.

Then you should continue by presenting the type of data you usually collect.

Our organization may process the following personal data on its employees:*

IMPORTANT: make sure you design this paragraph by reflecting your national labor and data protection laws and regulations. This is just an illustration how it should look.

- **General data:** Name and surname, address, date and place of birth, sex, ID number, citizenship, health insurance identifiers,
- **Academic and professional qualifications**: level of education, foreign language skills, employment history, data enlisted in submitted CV within the recruitment process,
- **Financial data:** bank account number, income data,
- **Information on work performance**: job title, supervisor assessment, business email address;
- **Communication data:** e-mail address, phone number, contact in case of an emergency.

Our organization may process the following personal data on its beneficiaries*:

IMPORTANT: make sure you design this paragraph by reflecting on your actual practices. This is just an illustration how it should look.

Name and surname, name of employer or the institution that the person represents, information on academic and professional qualifications, contact e-mail address, phone number.

If you provide legal aid to sensitive categories of clients, you should design this paragraph accordingly (for example: we collect information on the history of abuse and discrimination, information on sexual orientation, medical information.)

You could elaborate your practices on staff recruitment in similar fashion. Then you should provide concise information on:

For what purposes you process personal data.

- You collect information on your staff member to engage in labor relation, so usually the purpose is to meet mutual obligation arising from it.
- Usually you need data on your beneficiaries to conduct trainings, provide legal aid, etc.

The legal ground for processing personal data.

- Generally speaking, legal ground for contracting staff members is in national labor legislation.
- Usually the legal ground for collection of data on beneficiaries is established through their consent.

How personal data are being collected.

Here you should elaborate if you collect the data directly from data subjects, or through former employees, the agency you maybe contract to perform HR tasks for you, though organizations that delegate participants at your training, etc.

For how long will personal data be used.

- With regards to data collected on your employees, consult your national labor legislation. It probably establishes such deadlines. You should adhere to these rules and have them in your rulebook.
- Data on your beneficiaries should generally be stored until the purpose of its collection has been met. It does not necessarily end the moment you finish your training or provide legal aid. It is legitimate to store that data for some period of time, if you need to report them to your donors, or keep participants informed about your events in the future. But bear in mind that all of that should be timely communicated with beneficiaries and you need their consent for such practices.

The rights of data subject on the use of their data.

Here you need to enlist all the rights arising from your national data protection legislation and GDPR (if applicable). Typically, the rights of data subjects are:

- The right to be informed about data processing practices,
- The right of access to his/her personal data (usually, through a copy),
- The right to update inaccurate or incomplete information,
- The right to erasure data that are no longer needed or unlawfully processed,
- The right to withdraw consent,
- The right to restrict processing,
- The right to data portability.

Finally, the rulebook should contain information about the point of contact for any inquiries about personal data processing practices.

1.2 Introduce contract clauses with staff members (confidentiality and privacy clauses)

Your staff members should be timely informed about the rules of data processing in the office. You may want to consider amending contracts with your staff members by adding confidentiality and privacy clauses. Such clauses are usually explicit about responsibility of a staff member to use information and data in lawful and professional manner, in accordance with internal rules of the organizations that are usually elaborated in an internal rulebook.

For example:

"You are required to apply data processing rules and guidelines defined in the internal rulebook of the organization.

You are required to apply an appropriate standard of confidentiality of information and use personal data in lawful manner.

Any disclosure of confidential information belonging to the organization, or disclosure of personal data collected on behalf of the organization, kept on computer or other media, made unlawfully outside the proper course of duty will be treated as a disciplinary offence.
Any disclosure of personal data or confidential information to any unauthorized natural or legal person will lead to disciplinary action."

You may want to introduce such clauses in contracts with your permanent staff members, part time contracted associates, external consultants, volunteers, interns, and basically, any person you cooperate with that may have access to personal data your organization is responsible to process in lawful manner.

1.3 Develop Privacy Policy at the web site

Ok, we know that not many people read privacy policies. It is understandable. We visit so many different websites. Privacy policies are usually long (therefore – time consuming) and boring (therefore – not worth of reading). We don't have enough time to read and understand them all.

But keep in mind that they exist for a reason. They provide information about data processing practices that may occur while visitors use a web site.

You may consider using standardized version of Privacy Policy and to provide its summary in a more attractive form. For example: develop a table to provide answers to following questions:

Q	A
Do we use cookies?	Y/N
Do we use Google Analytics?	Y/N
What kind of data we use if our visitors want to submit a comment?	E.g. pseudonym, email, IP address
What kind of data we use if our visitors want to donate/support our organization?	E.g. credit card number, name and surname, etc.

Try using any other visuals that would clearly demonstrate your practices.

Search online for "privacy nutrition label" and see it anything you find there fits your organization's style of communication with the general public. By using privacy nutrition label approach to the design of your privacy policy, you may present information more quickly and in an interesting manner, so that visitors may eventually want to learn more about your practices.

1.4 Apply data protection rules when recruiting new staff members

Yes, you are hiring! It's a good news as it usually means your organization is growing. However, recruitment process requires that you use all those applications wisely.

- Include a reference on your rulebook in the job vacancy and invite candidates to read the document.
- Consider using a standardized CV template that could be downloaded, so that you eventually obtain the same categories of information.
- If you don't use standardized version of CV, instruct job candidates not to provide data that are not pertinent for the job vacancy. Which they sometimes do. You may want to include the following note:

Our organization does not use standardize template of CV. When submitting your CV, make sure to present information that are relevant for the job vacancy only.

- Establish internal rules on how long you plan to keep unsuccessful applications.

You could delete them immediately after you make a decision to hire someone else. But you may have a legitimate need to keep the application for a while if your organization keeps on growing and opens up new vacancies soon. So,

- Determine the time limit for keeping job applications (e.g. 2 years),
- Inform job candidates about that rule by acknowledging it in the job vacancy,
- Make sure you are really able to delete applications after the envisaged period of time wherever they may be at that time.

Before you start collecting job applications, make sure to:

- Designate only one e-mail for candidates to submit applications,
- Define who should have access to job applications (e.g. office manager, program officer, director, selection committee, or similar.)
- Restrict access to that e-mail for persons responsible for the process,
- If you print applications, keep them in the same folder and make them available only to designated staff members.

1.5 Define users' roles in your organization

Youth organizations usually do not have a lot of staff members. But certainly there is some type of division of labour and responsibilities. So, not all your staff members should have access to all categories of personal data the organization possess.

For example:

- Program staff probably does not need to have access to staff members' bank account numbers. Access to bank numbers should be restricted to financial manager, whoever is in charge of signing payment documents, accountant, etc.
- Project assistant working on one project may not need to have access to all personal data of consultants contracted through another project.
- Volunteers probably should not have access to confidential information about persons to whom you provide sensitive legal advice.

We know that you need to make sure the organization runs smoothly. But still you should determine which team member typically needs access to which categories of data.

- Design such rules internally, taking care of both legitimate needs - that the working process should not be hindered due to unreasonable restrictions, and the need to apply data protection standards.
- Communicate the rules with all staff members.
- Evaluate the rules from time to time. They should not be set in stone, especially if you see they could be improved.

Ok, so now let's move to the categories of data you collect through your project or program-based activities.

2. Project data and program operations

2.1 How should a YO use personal data when drafting project proposals?

In the fundraising activities you collect, you may sometimes need to provide the names of experts and other individuals you tend to hire through the project. Make sure to obtain their consent for that. This is not just a matter of fair business practices, it is a personal data issue as well.

- Provide full information to them about how their names (and other data) will be used in the project application.
- Avoid informing them through phone call; make sure you have their consent in your emails.

Ok, let's now assume your project has been supported and you start with the implementation. There are some beneficiaries you will interact with and that usually means you need at some of their data.

2.2 Obtain consent for data processing from your beneficiaries

Whenever you want to collect data from an individual, always:

- **Provide all relevant information** about data processing practices,
- Provide information prior to data collection,
- **Obtain consent** for such data processing practices.

We will further explore a few typical activities you implement, and leave you to apply same principles in other similar occasions.

A. Consent from applicants for trainings you organize

If you are organizing a training for which participants should fill in and submit application sheet, you should provide information about your practices in the application sheet.

You could use the following language in the notice, but **make sure it reflects actual practice:**

Information about our data processing practices:

*Through this application we collect the following personal data: name, surname, the organization you represent, e-mail, phone number.**

***enlist all categories of data you collect**

We collect data for the following purposes:

- *To timely inform participants about the event,*
- *To issue certificate of attendance,*
- *Promote future events to participants.**

***enlist all purposes you find legitimate. Remember, you are not allowed to change the purpose once you obtain consent, without new consent.**

Make sure to collect personal data that are necessary for the purposes you want to achieve. For example:

- If you want to issue a certificate, you probably don't need participants' home addresses.
- If you want to promote future events, you probably don't need date of birth.

This approach is called data minimization. **Don't collect the data you don't need.**

You could also provide the following information:

We will not use your data for any other purposes.

We will use your data in lawful and confidential manner. Access to your data is limited our team members who need the data to perform their tasks to meet the purposes of data processing.

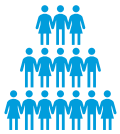
The legal ground for processing your data is your consent. By submitting the application form to us, you consent to the conditions of data processing elaborated here.

The consent you provide is freely given. You have the right to withdraw your consent.

You have the right to request additional information on how we use your data, which you can do by contacting as at: [provide contact e-mail].*

We advise you to see the Rulebook on Personal Data Protection at: [provide link to the document]

B. Consent from participants at events you organize



When you need participants lists to be filled in at your events, provide concise information about your data processing practices. You could use the following statement at the bottom of each side of the participants' list.

Our organization [name of the organization] collect your data to keep you informed on upcoming events within the project and to report to the donor [name of the donor] on implementation of the project. We will use your data in lawful and confidential manner. For more information contact us at: [contact e-mail].*

*** make sure to include all purposes for data processing, because you are not allowed to change it without prior consent.**

2.3 How to promote YOs' work at social networks?

YOs should promote their work. However, let's focus on some inadequate practices of promotion and see how you could avoid them.

Some participants may be put at risk if you promote the event

- Be extra careful if you organize event for members of social groups that are particularly exposed to discrimination, violence, or any violation of their civil or minority rights.
- Avoid posting visitors' photos at public events on sensitive issues (e.g. LBGT rights). Use panelists' photos instead.
- If you still need to publish photos from such events, try not to make visitors identifiable. Take the photo of a crowded room from the gallery, standing behind the visitors so that their faces remain hidden.
- If you are organizing international event on human rights issues, do not expose participants from non-democratic countries. Do not publish a photo of a member of LGBT community coming from a country in which same sex relation is punishable under the law. Remember, they need to go back home and someone may cause them harm.

Do not assume participants at your events would love you to publish photos!

If the event is closed to the public, there are no media, etc, you should:

- Before the event starts, inform participants that you want to make photos,
- Inform them about the purpose of it (e.g. reporting to the donor, promotion of the event),
- Ask participants if they are ok with:
  - Making photos,
  - Publishing photos.
- Obtain consent before you make photos and before you post them online.
- Don't exclude participants that don't want to be photographed. Respect their privacy-related decision.
- Publicize photos of persons that explicitly consented to that only.

Publishing case studies and personal testimonies may sometimes harm your beneficiaries

Some organizations publish case studies based on psychological support or legal aid they provide to their clients. Storytelling has become very popular way of promoting the work of YOs and has proven to be an effective way to get readers' attention, alarm media, and influence decisions makers. This is ok, as long as you apply data protection rules when you report on experiences of others.

Make sure that you always obtain that person's consent before publishing it.

- Provide full information to that person about your intentions to go public with the story.
- Inform that person on the amount of information you want to publicize.
- Make sure that person consents with the use of his/her real name.
- Be extra careful with publishing sensitive data (e.g. on victims of domestic violence, discrimination based on sexual orientation, etc) and obtain explicit consent for publishing such information from that person.
- If the person wants to go public, be sure that the person understands what is his/her role in the campaign.
- If he/she opposes to the disclosure of personal data, respect that decision.
- In such case consider using pseudonym.
- In such case make sure that you do not publicize any information that may ultimately identify that person. E.g. avoid mentioning the village of residence, where he/she works, etc.
- In such case if you think a video testimony would make a difference, blur the face and distort the sound.
- Limit access to raw materials, keep it confidential and inform team members on disciplinary consequences in cases of misuse of the materials.

2.4 How should a YO use its beneficiaries' data when reporting to its donors?

Ok, your project has been successfully implemented. Now it's time to draft and submit report to your donor.

Donors are sometimes quite demanding, but their interests are legitimate. They need proof that activities that they support have been implemented. Other than narrative reports, they may request documents developed within specific activities, e.g. intake forms when you provide legal aid to your clients, photos taken at closed meetings, participants' lists, etc.

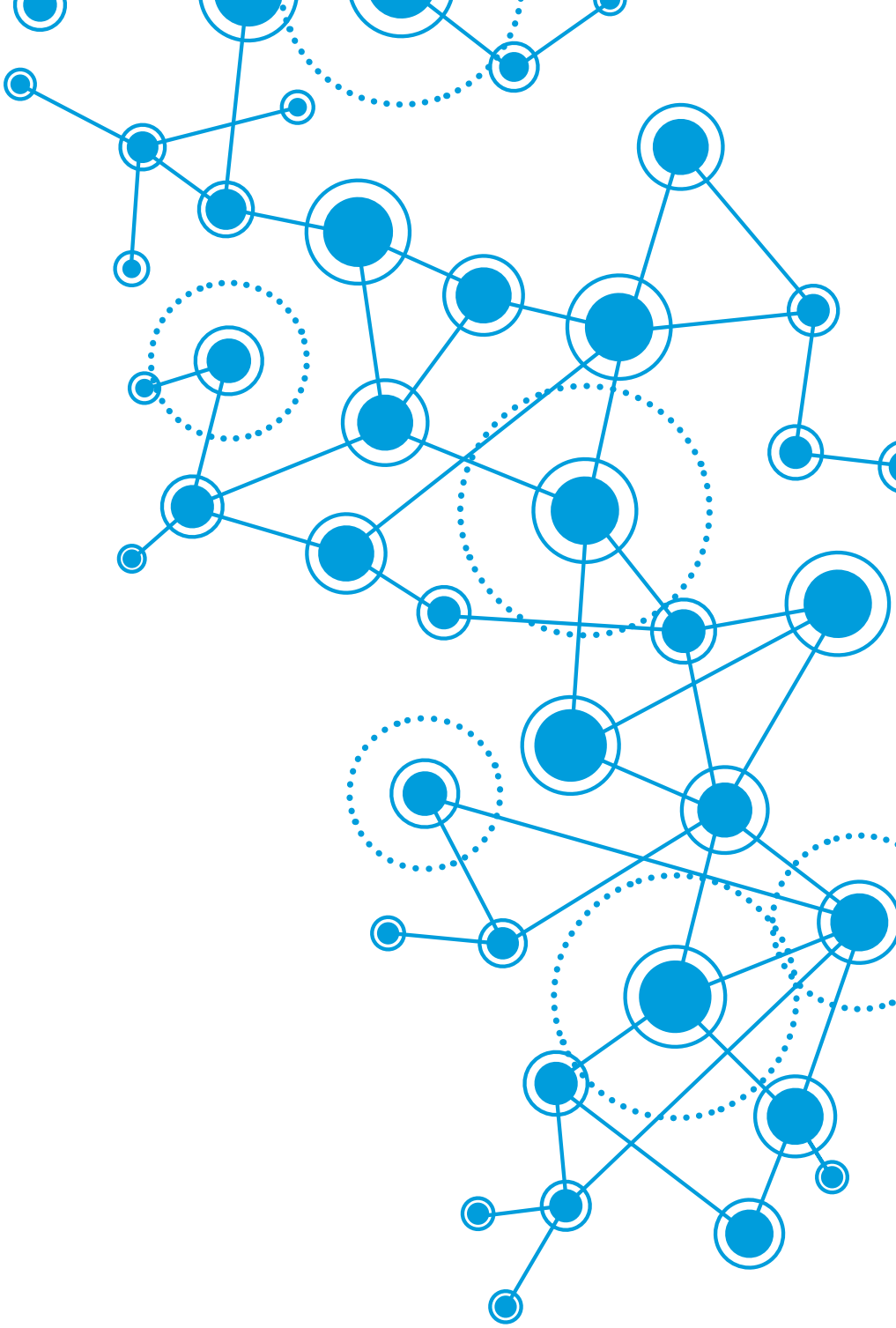
Make sure to clarify reporting rules with the donor **when you start implementing the project** if you recognize possible privacy-related concerns. That may occur in particular if you anticipate you will collect sensitive personal data on:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- medical data
- individual's sex life or sexual orientation.

Here are some steps you could take to be on the safe ground:

- Inform the donor on sensitive issues within the reporting process.
- Clarify with the donor if all documents containing personal data should be fully reported.
- If they need to be reported, apply anonymisation when reporting on sensitive issues (e.g. intake forms you develop while providing legal aid to victims of discrimination). Make sure not to provide information that may lead to identification of that person.
- Whatever the rules of the donor are put in place, inform data subject about your relation with the donor and how the data would be processed.
- Obtain consent from data subject for reporting to the donor.
- Apply data minimization principle as much as possible, through limited collection of data from the client.

Also, some donors request you to provide payment lists, to demonstrate that you have used the money properly. Bank statements usually consist of several payments. When submitting bank statements to donors, make sure to use black marker to hide payments that are not supported by the donor you report to.



The purpose of these advises is to assist you to become more digitally safe. But bear in mind that the advices do not necessarily cover all your data processing practices. They are designed to be guidelines that you need to adapt to your working environment.

Good luck!

This publication was produced by CONNECT International with the support of the European Youth Foundation of the Council of Europe. It does not necessarily reflect the official position of the Council of Europe.

For publisher: Connect International AISBL
Within the projec: UpDatAed – toward digitally safe youth organizations
Design and print: Agency Pro22
Circulation: 1500
Year: 2019