Co-funded by
the European Union

PROTECT

PROTECT TOOLKIT

PRACTICAL PRIVACY, DATA PROTECTION, AND DIGITAL SAFETY GUIDANCE FOR YOUTH WORKERS AND YOUTH ORGANISATIONS

PROTECT Toolkit

Practical privacy, data protection, and digital safety guidance for youth workers and youth organisations

Every year, youth organisations across Europe run youth exchanges, training courses, local workshops, participation projects, volunteering activities, and cross-border partnerships that involve large numbers of young people, youth workers, trainers, and partner institutions. Within the wider Erasmus+ programme alone, more than **34,400 projects** were supported in 2024, involving over **85,600 organisations** and providing learning opportunities to almost **1.5 million participants.**

This scale matters because each project generates personal data from the moment outreach begins. Registration forms, attendance lists, travel arrangements, accommodation planning, emergency contacts, accessibility requests, dietary information, photos, videos, certificates, follow-up communication, and online collaboration tools all involve the collection, use, storage, or sharing of personal data. Erasmus+ also confirms that the programme includes mobility, project, and funding activity on a long-running and programme-wide basis, showing that these data-processing practices are not occasional but structural to the sector.

The need for proper data handling becomes even more important when considering who takes part in these activities. In 2024, Erasmus+ supported almost 265,000 people with fewer opportunities, including migrants, persons with disabilities, people living in remote areas, and people facing socioeconomic difficulties. This means that many youth projects do not handle only basic contact details; they may also process more sensitive information linked to health, accessibility, support needs, or social vulnerability.

For youth organisations, handling personal data properly is therefore not an administrative side issue. It is part of safeguarding, trust-building, and professional responsibility. A registration list sent to the wrong recipient, an image shared without valid permission, or support information stored in an uncontrolled folder can expose young people to embarrassment, discrimination, exclusion, or actual harm. Erasmus+ projects are implemented through large numbers of organisations and cross-border partnerships, and this creates repeated situations where data is shared, stored, and reused across teams, platforms, and countries. In that environment, proper handling of personal data is essential not only for GDPR compliance, but alsofor clear project management, responsible partnerships, and credible accountability toward participants, parents, funders, and public authorities.

In short, the more youth work becomes international, digital, and collaborative, the more important data protection becomes. Youth organisations do not need to become law firms, but they do need to become competent and disciplined stewards of the personal data entrusted to them. Handling personal data properly is now part of what it means to run a safe, ethical, and trustworthy youth project in Europe.

What this toolkit helps you do

- collect only the data you really need
- explain clearly why you ask for personal data in the youth projects
- separate necessary participation data from optional permissions
- handle photos, newsletters, and partner sharing safely
- store, review, and delete data in a disciplined way

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Inside this toolkit	Best used by
Introduction and 5 practical chapters, standard templates, checklists, worksheets, and ready-to-run lesson pages	Youth workers, project coordinators, trainers, NGO staff, and volunteers

Before you start, ask five questions about your current work practices in youth programs and mobilities:

- What am I collecting?
- Why do I need it?
- Who will see it?
- How long will I keep it?
- How will I protect it?

How to use this handbook

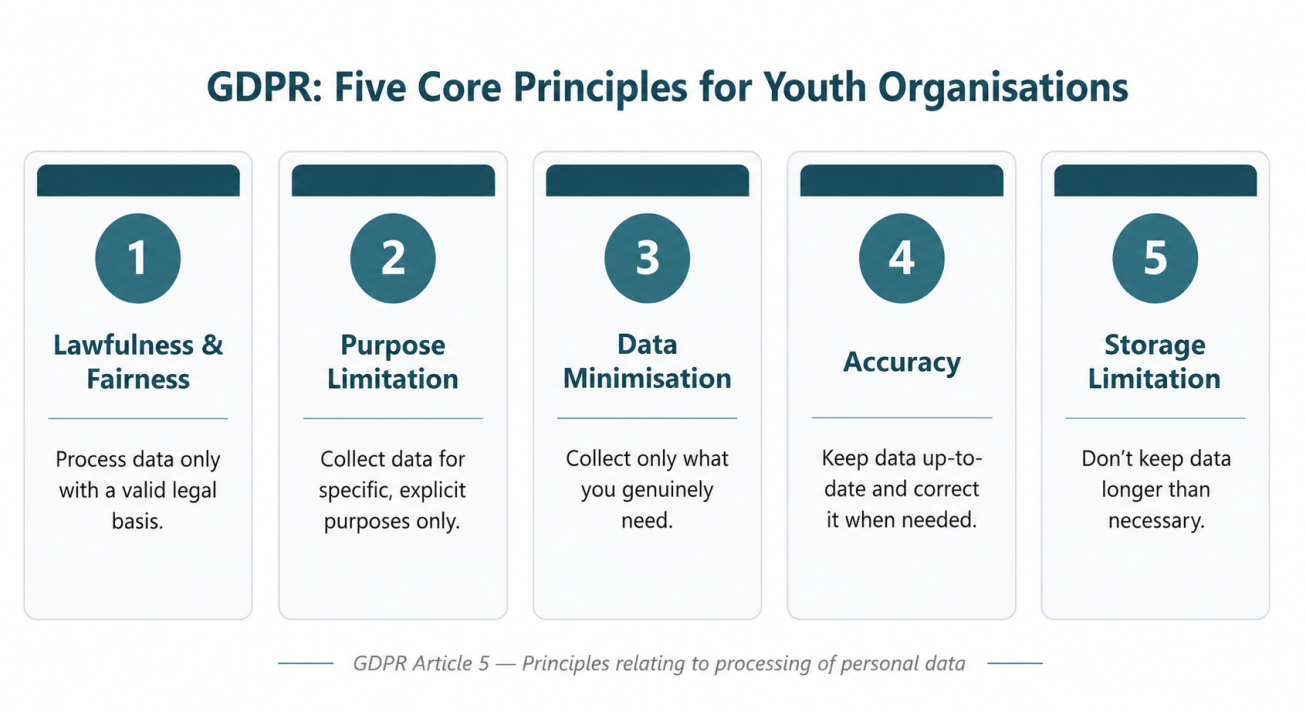
This toolkit is meant to save time. You do not need to read it like a law book. Start with the chapter that matches the task in front of you. If you are preparing registrations, go to Chapter 3. If you are planning visibility or dissemination, go to Chapter 4. If you are cleaning shared folders after an activity, go to Chapter 5.

A simple working method

- Read the chapter intro first. It tells you what really matters in youth work practice.
- Use the checklists before you build a form, send a partner file, or publish content.
- Copy and adapt the templates instead of drafting from zero each time.
- Run the lesson pages as short staff sessions or volunteer briefings when your team needs common understanding.

The five rules behind the whole toolkit

- Explain before you collect. People should know what you need, why you need it, and what is optional.
- Collect less. Avoid the habit of asking for information just because a form has space.
- Separate purposes. Participation data, emergency information, newsletter sign-up, and photo permissions should not be bundled together.
- Control access. Personal data should be visible only to the people who genuinely need it for delivery, support, or compliance.
- Delete with intention. Keep what is required for reporting or audit, and remove what no longer has a clear purpose.



The five principles in practice

Principle	Why it matters	In practice
1. Be clear and fair	People should understand what you collect, why you need it, and how you will use it.	Explain before you collect. Use simple language in forms and conversations.
2. Collect only what you need	Ask only for the information that is necessary for the activity, support, or reporting.	Remove extra fields. Do not collect data just because it might be useful one day.
3. Use data only for the stated purpose	If you collected data for participation, do not reuse it for newsletters, publicity, or other purposes without a proper basis.	Keep participation, support, media, and follow-up purposes separate.
4. Keep data accurate and secure	Incorrect data can cause mistakes, and poorly protected data can expose participants.	Update important records, limit access, use secure tools, and protect devices and folders.
5. Do not keep data forever	Personal data should be kept only as long as it is genuinely needed.	Set retention periods, review files regularly, and delete what no longer has a clear purpose.

Quick note for Erasmus+ partnerships

In cross-border projects, privacy work is not only an internal office matter. It affects registrations, travel coordination, visibility, online collaboration, stakeholder mapping, reporting, and project outputs. That is why the partnership should agree early on who collects, who decides, who stores, who shares, and who answers participants when they ask questions about their data.

Chapter 1

Introduction & How to Use This Toolkit

Why this chapter exists

Privacy decisions happen before the first form is sent. They happen when you decide what information to ask for, how to store it, and who gets to see it. This chapter is designed to help everyone on the project team start from the same point. It explains who this toolkit is for, what it is built to solve, how to navigate it efficiently, and what the most important terms mean in everyday practice.

What you need to know

- This toolkit is for youth workers, coordinators, trainers, volunteers, and anyone handling participant data in Erasmus+ or other EU-funded youth projects.
- Privacy is not a barrier to effective youth work. Handled well, it makes your project more trustworthy and participant-centred.
- You do not need to be a legal expert. You need to understand what you are doing with data and be able to explain it clearly to others.
- Each chapter in this toolkit is self-contained. Start with the area most relevant to your current task.

Who this toolkit is for

The PROTECT Toolkit is written for staff and volunteers in youth NGOs, Erasmus+ project coordinators, trainers running sessions on digital safety and data literacy, and partner organisations in cross-border projects. It is not written for lawyers or data protection officers. It is written for the people who actually run activities, build forms, share photos, send newsletters, manage shared folders, and deal with participants face to face. If that is you, this toolkit is for you.

What problems it solves

Youth organisations in Europe regularly handle sensitive personal information under conditions that were not designed with GDPR in mind. Registration forms collect more than necessary. Photo permissions are bundled with participation agreements. Files are stored on personal devices or open cloud links. Partner organisations share data without a clear written understanding. After an activity ends, nobody deletes anything. These are real and common problems. This toolkit does not solve them with legal warnings. It solves them with practical tools, standard templates, and plain explanations that any team member can follow.

How to navigate this toolkit

You do not need to read this toolkit from beginning to end. Start with the chapter that matches the task in front of you. If you are building a registration form, go to Chapter 3. If you are planning photos or social media posts, go to Chapter 4. If you are reviewing your shared folders or setting a deletion routine, go to Chapter 5. If something has gone wrong, go to Chapter 6.

Within each chapter you will find a short introduction, a box of key points, practical guidance sections, a checklist, ready-to-use templates, and a lesson page designed for team training. Use what matches your current need and return to the rest when it becomes relevant.

Which template to use, and when

Use this quick map to jump straight to the right tools for the phase you are in. Every template is ready to copy and adapt.

Set-up -agree roles before any data is collected: Templates 1.1, 1.2, 2.1, 5.1, 5.2
Recruitment & registration -building forms, collecting data: Templates 3.1, 3.2, 2.2, 3.3, 3.6
During the activity -attendance, photos, sessions: Templates 3.4, 3.5, 4.1, 4.2, 4.6, 5.3

Communication & dissemination -newsletters, social media, partner sharing: Templates 4.4, 4.5, 4.3
Participant requests -someone asks about their data: Templates 2.3, 2.4
Close-out & incidents -cleaning up, or something goes wrong: Templates 5.4, 5.5, 5.2, 6.1, 6.2
The data journey -six project phases

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Set-up	Recruit	Activity	Communicate	Requests	Close-out

Key terms

- Personal data: Any information that can identify a living person directly or in combination with other data. Names, email addresses, photos, phone numbers, location data, and online identifiers all count.
- Data controller: The organisation or person who decides why personal data is collected and how it is used. In most youth projects, this is the lead NGO or the partner organisation running the activity.
- Data processor: An organisation or tool that handles personal data on behalf of the controller. A survey platform, a mailing list provider, or a cloud storage service may act as a processor.
- Lawful basis: The legal reason that justifies collecting or using personal data. Common examples are contractual necessity, legitimate interests, legal obligation, and consent. Consent is one option, not the default.
- Data minimisation: The principle that you should collect only the personal data you genuinely need for a specific purpose. If a field is not necessary, do not add it to the form.
- Retention: How long you keep personal data. Data should not be kept longer than necessary for the purpose it was collected for, or longer than required by applicable audit or grant rules.
- Data subject rights: The rights that individuals have over their personal data, including the right to access it, correct it, and in some cases delete it or object to its use.
- Privacy notice: The information you must give to participants when you collect their data, explaining what you collect, why, who sees it, how long you keep it, and how they can exercise their rights.

Chapter 1 checklist

- Does your team have a shared understanding of what personal data means in the context of a youth project?
- Is there a named person responsible for privacy coordination in your organisation?
- Have you identified which chapters of this toolkit are most relevant to your current project phase?
- Have you shared the key terms in this chapter with any staff or volunteers who handle participant data?

Templates and worksheets

Template 1.1 - Project privacy contact card

Purpose: Establish a clear single point of contact for any privacy question in your project.

Use when: At project start and whenever a new partner joins or a role changes.

Completed by: Project coordinator, distributed to all partners.

Organisation name: [Full name of the organisation]

Privacy contact name: [Name of the person responsible for privacy questions]

Privacy contact email: [Email address]

Backup contact: [Name and email of a second person if the primary is unavailable]

Scope: [Activities or data processes this organisation is responsible for]

Data types handled: [Registrations / photos / mailing lists / partner data / other]

Use note: Share this card with all project partners at the start. Update it if roles change during the project life cycle.

Template 1.2 - Quick-start guide by role

Project coordinator: Start with Chapter 2 for the legal basics, then Chapter 5 for storage and retention planning.

Activity organiser: Start with Chapter 3 for participant data collection and Chapter 4 for photos and communication.

Trainer or facilitator: Start with the lesson pages at the end of each chapter and Chapter 1 for key terms.

Volunteer: Start with Chapter 3 for registration guidance and Chapter 6 for what to do if something goes wrong.

Use note: Print or share this guide at the first team meeting and again before major activity phases.

Lesson page - Privacy in everyday youth work

Aim Duration Group size Materials

Build shared privacy literacy and identify role-specific priorities. 40 to 50 minutes 4 to 20 people This chapter printed, scenario cards, and a flipchart

Step-by-step flow

1 5 min Open with a quick question: name one moment in the last project where you handled someone's personal data. Collect answers without judgement.

2 10 min Walk through the key terms in this chapter. Invite examples from the group for each term. Correct only where clearly wrong.

3 10 min Split into pairs. Each pair picks one scenario card and decides: who is the controller? what is the lawful basis? what would they tell participants?

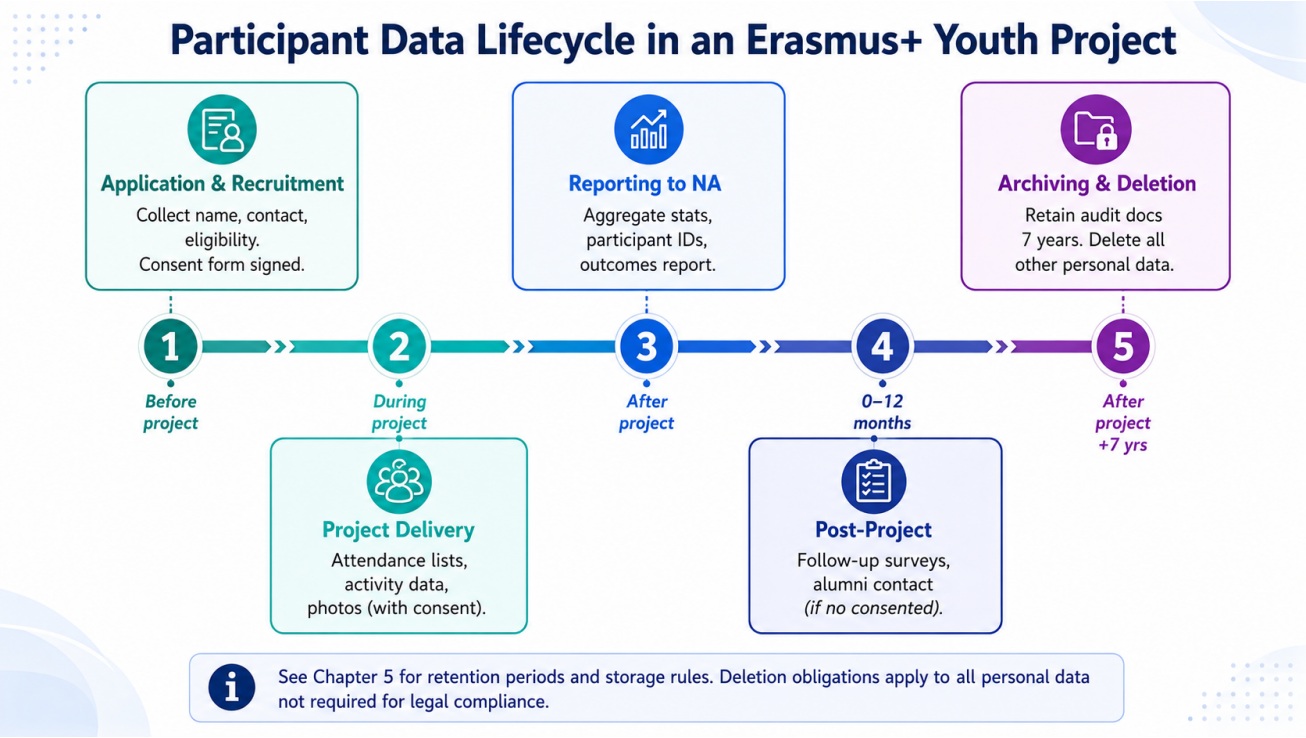
4 10 min Debrief in the full group. Agree on one shared principle the team will apply going forward.

5 5 min Close by identifying the one chapter each person should read first based on their role.

Debrief questions

- Which privacy decision did we realise we had been making incorrectly?
- What is the single change we can make this week to handle data better?
- Who in this team still needs a clearer understanding of their role?

Key message: Good privacy practice is a team habit, not an individual responsibility.



Chapter 2

GDPR Basics for Youth Projects

Why this matters in youth work

Youth workers handle personal data almost every day, even when they do not think of it in legal terms. Registration forms, attendance sheets, partner lists, travel details, group chats, mailing lists, photos, and workshop feedback all involve decisions about people's data. If those decisions are unclear, the project becomes harder to manage and trust becomes easier to lose. This chapter gives you the practical foundations you need before you build any form or share any participant information.

By the end of this chapter, the reader should be able to:

- understand what **personal data** means in the everyday reality of youth projects
- distinguish between general personal data and special category data
- explain in simple terms the difference between a **controller**, **processor**, and **joint controller**
- identify which organisation is responsible for different data processes in a partnership
- understand that consent is not the legal basis for everything
- recognise the main **participant rights** and know what the organisation should do when a request is received
- feel more confident when discussing basic privacy responsibilities with colleagues, partners, or participants

How this helps in practice

This chapter helps youth workers build a strong foundation before they start creating forms, sharing files, or planning activities. It gives them the vocabulary and confidence to understand who is responsible for what, avoid common misunderstandings, and make better day-to-day decisions from the start.

What you need to know

- Personal data is not only names and email addresses. It also includes photos, phone numbers, IDs, online identifiers, and combinations of details that can point to one person.
- The most important starting question is who decides why and how the data is used. That usually tells you who the controller is.
- Consent is not the answer to every situation. Many project tasks rely on other lawful bases, and consent should not be used as a shortcut.
- Participants have rights, and your organisation needs a simple route for receiving and answering requests.

Strong takeaway: if your team cannot explain who is responsible, why the data is being used, and what rights route the participant has, your process is not ready yet.

Legal anchor: GDPR Articles 4, 5, 6, 12-15, 21; EDPB Guidelines 07/2020 on controller and processor concepts; Erasmus+ Programme Guide Part C

What counts as personal data in a youth project

In youth work, personal data often appears in ordinary practical materials. A participant application form contains direct identifiers. A photo gallery may show identifiable faces. A spreadsheet with travel details can reveal names, routes, accessibility needs, and accommodation arrangements. A WhatsApp group with phone numbers is also processing personal data. The safest habit is to assume that if information links to a real person, and your team can use it to contact, recognise, support, or distinguish that person, you should treat it as personal data.

It helps to separate **general personal data** from **special category data**. General personal data is the ordinary information most youth workers handle every day. It includes names, email addresses, phone numbers, dates of birth, travel details, room allocations, signatures, certificate records, photos, and contact lists. This kind of data still needs care and a clear purpose, but it is not automatically treated as sensitive under GDPR just because it is personal.

Special category data is a smaller and more sensitive group of information that receives stronger protection. Under GDPR, this covers data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, data concerning health, and data about a person's sex life or sexual orientation. In practice, youth organisations should assume that this type of data

needs an especially strong reason for collection, tighter access control, and more careful storage and deletion routines.

In youth projects, special category data often appears in practical support fields rather than in formal legal language. An accessibility request may reveal health information. An allergy or medication note is health data. A dietary request may stay general if it is just a meal preference, but it can become more sensitive if it reveals an allergy, a medical condition, or a religious belief. This is why youth workers should never collect "extra details just in case". They should ask only for what is truly needed to support safe and inclusive participation (seek only information that is essential for the type of activity you are organizing).

Is it general data or special-category data?

General personal data -everyday info, still needs care	Special category data -extra care: stronger reason + tighter access
Name	Health / allergies
Email	Religion
Phone number	Ethnic origin
Photos	Biometric data
Travel details	Sexual orientation
Room allocation	Political views

Common Erasmus+ examples
- participant and trainer application forms
- lists with names, dietary needs, and room allocations
- travel booking information and boarding pass copies
- sign-in sheets, certificates, and Youthpass-related participant records
- photos, videos, interviews, testimonials, and partner dissemination materials
- stakeholder contact lists and community mapping spreadsheets

Controller, processor, and joint controller in practical language

Who decides?

Role	What it does	Example
Controller	Decides why and how.	"We chose what to collect"
Processor	Acts on instructions only.	A form tool or print supplier
Joint controllers	Decide together.	Partners co-design the form

Controller = the one who decides (why the data is used and how the process works)

Processor = the one who helps (handles the data for someone else and follows instructions)

Joint controllers = two or more organisations decide together

The three roles in detail

Role	What it decides or does	Key obligation
Controller	Decides why data is collected, what data is collected, how it will be used, and who can access it.	Responsible for compliance and for responding to people.
Processor	Processes data only on instructions; does not decide the purpose or what happens with the data.	Must follow the controller's instructions and keep data secure.
Joint controllers	Two or more organisations decide together why data is collected, what data is collected and how it will be used.	Share responsibilities and must have a clear arrangement.

Quick memory trick: controller = decides · processor = follows instructions · joint controllers = decide together.

A controller decides the purpose and main means of processing. In simple language, the controller answers the questions: Why are we using this data, and how will the process work? A processor handles data on the controller's behalf. A platform storing your form responses may be a processor. In partnerships, things become more delicate. If two or more organisations decide together why and how the data will be used, they may be acting as joint controllers. That is common when partners jointly design registrations, define participant selection, plan visibility, or manage shared reporting arrangements.

A very easy way to test it is to ask:

- Who decided why this data is needed?
- Who decided what data will be collected?
- Who decided what will happen with it?

If one organisation makes those decisions, it is usually the **controller**.
If another organisation only handles the data on its instructions, it is usually a **processor**.
If two or more organisations made those decisions together, they may be **joint controllers**.

For example:

- If your organisation creates the registration form and decides what must be collected, it is likely acting as **a controller for that stage**.

- If a partner only receives a limited participant list because it needs to arrange accommodation or local hosting, that does not automatically make it the sole controller for the whole process.

- If the consortium decides together what participant data will be collected, how long it will be kept, and which channels will use it, **a joint-controller discussion is usually needed**.

Examples from youth project work

Scenario	What happens	Roles
One NGO creates a registration form	The NGO decides what data is collected and why.	Controller: NGO · Processor: form platform
A partner only shares the registration link	The lead partner creates the form; the other partner only shares the link.	Controller: lead partner · Local partner: not a processor
Two partners design the form together	Both decide what data is collected and how it will be used.	Joint controllers: partner A and partner B
An external company prints certificates	The company prints certificates on the organiser's instructions.	Controller: organising NGO · Processor: certificate company
A hotel receives a rooming list	The hotel uses data for check-in, invoicing and legal duties.	Controller: hosting partner · Hotel: its own controller (not a processor)
A mailing list platform sends newsletters	The NGO collects opt-ins and uses the platform to send emails.	Controller: NGO · Processor: email platform
A photographer takes pictures	The photographer works on the organiser's instructions and delivers the files.	Controller: partner organisation · Processor: photographer (if acting only on instructions)
A shared spreadsheet for travel arrangements	The partners agree together what data is needed and how it will be used.	Joint controllers: lead partner and hosting partner
A volunteer posts health details in a group chat	The volunteer shares data in a group; the organisation is still responsible.	Controller: organisation · Volunteer: acts under its responsibility
Each partner posts the video on its own social media	Each partner decides independently to publish on its own channels.	Controller: each partner for its own publication

Practical rule for partnerships

Do not leave role questions vague. Write down who collects the data, who stores it, who answers rights requests, who publishes images, and who removes content if someone objects or withdraws permission later.

Ultra-simple test: ask three questions

– Who decided why we need this data?

– Who decided what we collect?

– Who will answer if a participant asks about their data?

If one organisation answers all three, it is likely the controller. If another only helps, it is the processor. If two or more answer together, they may be joint controllers.

Note: not every recipient is a processor. Some recipients (e.g. hotels, airlines, banks, insurance companies) act as their own controllers because they use the data for their own purposes.

Tip: when in doubt, write it down, agree it with your partners, and explain it to participants in clear and simple language.

Lawful bases in practice

One of the most frequent mistakes in youth projects is treating consent as a universal permission slip. In reality, if data is necessary to organise participation, communicate practical information, support travel, or meet reporting duties, consent may not be the right lawful basis. Consent works best for genuinely optional uses, especially public communication or newsletter sign-up. If a participant might feel they have to say yes in order to join the activity, the consent is unlikely to be freely given.

- Use a necessity-based approach for the data that is required to run the activity itself.
- Use separate and clearly optional consent for newsletters, testimonials, or some types of public communication.
- Never hide optional permissions inside a mandatory registration block.
- Always make withdrawal easy where you rely on consent.

Working with non-EU partners

Many Erasmus+ projects involve partner organisations from Western Balkans countries such as Serbia, North Macedonia, Bosnia and Herzegovina, or Albania. It is important to understand that GDPR does not apply directly in these countries. Their own national data protection laws govern how data is handled on their side. When your EU-based organisation shares personal data with a non-EU partner, you are responsible for ensuring the transfer is protected. This typically

means including a data protection clause in the partnership agreement and transferring only the minimum dat necessary for the partner's specific task. If data regularly flows between EU and non-EU partners, consider seeking specific data protection advice for your country and the partner countries involved. Do not assume that because a partner is trustworthy and well-intentioned, the legal framework around the transfer takes care of itself.

Participant rights and response discipline

Participants have the right to ask what data you hold, to correct it, and in some cases to ask for deletion, restriction, or objection. What matters in practice is that your organisation has a visible contact point and a calm internal process. Youth workers do not need to memorise every legal article. They do need to know where the request should go, who checks identity if needed, and who signs off on the reply.

Minimum response routine

- acknowledge the request quickly
- log the date of receipt
- check which team member owns the response
- verify identity only where needed
- reply clearly and within the expected timeframe

Chapter 2 checklist

- Can we explain in one sentence why we are collecting each category of data?
- Do we know which organisation is acting as controller for each main processing step?
- Have we avoided using consent for data that is actually necessary for participation?
- Is there a clear privacy contact email or responsible person?
- Do staff know what to do if a participant asks for access, correction, or deletion?

Templates and worksheets

Template 2.1 - Roles and responsibilities worksheet

Purpose	Use when	Completed by
Map who decides, who handles, and who responds in each data process.	At project start, before registrations, or when a new partner joins the workflow.	Coordinator together with the relevant project partners.

Activity or process	[Registration / travel / hosting / visibility / reporting / stakeholder mapping]
Lead organisation	[Name of organisation]
Why is data used	[Short description of purpose]
Who decides the fields or purpose	[Organisation / role]
Who stores the data	[Folder, platform, or tool owner]
Who can access it	[Roles only, not broad groups]
Who answers participant questions	[Email / responsible person]
Delete or review date	[Date or retention rule]

Use note: Use one worksheet per process. Do not try to fit the whole project into one generic note.

Template 2.2 - Participant privacy notice

Purpose	Use when	Completed by
Give people the core information they need when their data is collected.	Before or at the point of collection, especially in registration forms and workshop sign-up processes.	The controller or lead organisation collecting the data.

Privacy Notice for Participants

We are collecting your personal data to organise and deliver this activity, communicate practical information, provide support where needed, and meet any relevant reporting or audit duties connected with the project.

We collect only the data that is necessary for these purposes. Some fields may be optional. Where something is optional, you can decide freely whether to provide it.

Your data may be accessed by authorised staff from the project partners and, where necessary, by service providers that help us deliver the activity. Data is shared only on a need-to-know basis.

We keep your data only for as long as it is needed for the purposes explained to you, and for any period that is required by reporting, compliance, or audit rules.

You have the right to ask for access to your data, correction of inaccurate data, and in some cases deletion, restriction, or objection. If we rely on your consent for an optional use, you can withdraw that consent at any time. For privacy questions, please contact: [Email] [Organisation name]

Use note: Adapt the recipients, international transfer information, and retention wording to your real process.

Template 2.3 - Rights request log

Purpose	Use when	Completed by
Track requests and keep your team organised.	Whenever a participant asks for access, correction, deletion, restriction, or objection.	The person responsible for privacy coordination.

Request ID	[Internal number]
Date received	[DD/MM/YYYY]
Name of requester	[Name]
Type of request	[Access / correction / deletion / restriction / objection / other]
Identity check needed	[Yes / No and how]
Owner of response	[Name / role]
Deadline for reply	[Date]
Outcome	[Completed / refused / partially fulfilled]
Notes	[Short factual note]

Template 2.4 - Rights request acknowledgement

Purpose	Use when	Completed by
Confirm receipt and set a calm, professional tone.	Immediately after receiving a request.	The person who monitors the privacy contact channel.

Subject: Your request about your personal data is received Hello [Name],

Thank you for contacting us. We confirm that we received your request on [date].

We will review your request and reply without undue delay. If needed, we may ask you to confirm your identity before we disclose, change, or delete personal data.

If the request is complex, we will explain the next steps to you clearly.

Kind regards,
[Name]
[Organisation]

Lesson page - Who decides what?

Aim	Duration	Group size	Materials
Help staff distinguish between controller, processor, and joint-controller situations.	30 to 45 minutes	6 to 20 people	Printed scenario cards, sticky notes, and one flipchart

Step-by-step flow in case you need to execute this activity in your project

Step	Time	What to do
1	5 min	Briefly explain the difference between deciding the purpose and simply handling data on someone else's behalf.
2	20 min	Give the group three or four project scenarios, such as registrations, accommodation booking, newsletter sign-up, or photo publication. Each group will read scenarios. Their task is not to solve every legal detail, but to answer four practical questions: Who is the controller? Is anyone acting only on instructions, like a processor? Are two organisations deciding together? Who should answer if a participant asks about their data?
3	10 min	Ask groups to explain their reasoning in one minute only. Review each scenario together and discuss where teams often become confused in real projects.
4	5 min	Ask each participant to name one process in their organisation that needs clearer role definition.
Debrief questions		

- Who decided why the data would be used?
- Which organisation shaped the form, the purpose, or the sharing plan?
- Who would the participant contact if they wanted an answer tomorrow?

Chapter 3

Collecting and Using Data in Practice

Why this matters in youth work

A well-run youth activity usually starts with a form, a sign-up process, or some other practical way of gathering information. This is the stage where many privacy problems begin. Teams ask for too much, mix necessary and optional information, or collect sensitive details without planning who will see them. This chapter helps youth workers design cleaner forms, give clearer explanations, and handle support information with care.

By the end of this chapter, the reader should be able to:

- design or review a participant form using the principle of **data minimisation**
- distinguish clearly between **mandatory** and **optional** fields
- explain the purpose of data collection in a way that participants can easily understand
- collect support-related information, such as health, dietary, or accessibility needs, in a safer and more limited way
- avoid collecting unnecessary or overly detailed personal information
- recognise when extra care is needed for the data of **minors**
- separate participation requirements, support needs, and optional permissions in a clearer and more respectful way

How this helps in practice

This chapter helps youth workers improve one of the most common and risky parts of project work: collecting information. It makes registration forms shorter, clearer, and easier to justify. It also helps teams protect sensitive information better and reduce the chance of collecting data they do not really need.

What you need to know

- Every field on a form should have a reason that can be explained in plain language.

- Mandatory fields and optional fields should look different and behave differently.

- Sensitive information such as health, dietary, or accessibility needs should be collected only when necessary and handled with tighter access.

- Minors' data needs a careful approach that separates participation permission, safeguarding, and privacy-related permissions.

Strong takeaway: a good registration form is not the one that asks everything. It is the one that asks only what the project can justify and use responsibly.

Legal anchor: GDPR Articles 5, 6, 9, 12-14; European Commission guidance on data minimisation, consent, and information duties

Data minimisation in real life

Data minimisation means collecting information that is adequate, relevant, and limited to what is necessary for the purpose. In youth work, this principle is especially helpful because forms often grow by habit. Someone adds a field once, nobody removes it, and after a year the organisation is collecting much more than it can defend. The easiest test is simple. If your team cannot explain why a field is needed for this specific activity, the field should probably go.

Ask these three questions before you keep a field

- Does this field directly help us organise, support, or safely deliver the activity?

- Could we run the activity without this field?
- If a participant asked why we need this information, would our answer sound reasonable and clear?

Mandatory versus optional

Spot the problem

A registration form for a one-day local workshop asks every participant for their full home address, ID number, and a recent photo. What is wrong here?

Answer: almost none of it is needed for a one-day workshop. A name and an emergency contact are usually enough. If you cannot explain why a field is needed, leave it out.

Youth workers often need some information to run an activity properly. Names, contact details, travel needs, and emergency contacts may be necessary. Other things are useful only for future communication or visibility. These should be placed in separate optional sections. This protects the participant's freedom of choice and also makes your process easier to explain.

- Do not hide newsletter sign-up inside the same confirmation line as registration.
- Do not ask for a testimonial or public quote inside a mandatory application block.
- If an answer is optional, say so directly next to the field.
- If a field is optional because it helps inclusion or support, explain that clearly too.

Why we ask different categories of data

Not all participant data serves the same purpose. That is why a good youth project form should not look like one long list of questions. Different categories of data exist for different reasons, and each category should be asked, explained, stored, and reviewed in a slightly different way. This makes the form easier to understand, easier to justify, and safer to manage.

The main rule is simple - **group data by purpose**. When youth workers do this well, participants can immediately see what is necessary for joining the activity, what is asked only for support and safety, what is optional for future contact, and what is optional for visibility or dissemination. This reduces confusion, builds trust, and helps the organisation follow data minimisation in a practical way.

Necessary participation data

This is the core information needed to organise and deliver the activity. It usually includes things such as full name, contact email, phone number where needed, organisation, age group where relevant, and basic logistical details.

Why we ask it:

We ask this data because without it, the activity cannot be properly organised, participants cannot be contacted, and the team cannot manage attendance, travel, or delivery.

Instruction for youth workers:

Ask only for what is genuinely needed to run the activity. If the activity can happen without a certain field, remove it.

Support and inclusion data

This category includes accessibility adjustments, dietary needs, mobility support, allergy-related notes, or other practical information needed to support safe and full participation.

Why we ask it:

We ask this data to make participation safe, respectful, and inclusive. The purpose is not to collect personal details out of curiosity, but to understand what the team needs to do in practice.

Instruction for youth workers:
Collect only the minimum needed for support. Focus on practical instructions, not full personal or medical stories. Access should be limited to the people who truly need to know.

Emergency and safety data

This may include emergency contact details or short safety-related instructions that matter during the activity.

Why we ask it:
We ask this data to respond responsibly if something goes wrong during the activity and to protect participant well-being.

Instruction for youth workers:
Keep this category clearly separated from communication or visibility purposes. Do not collect more than the team would realistically use in an emergency.

Optional media and visibility data

This includes permission for identifiable photos, videos, quotes, testimonials, interviews, or public communication content.

Why we ask it:
We ask this because public visibility is not the same thing as participation. A project may need communication materials, but participants should have a real choice about whether they appear in them.

Instruction for youth workers:
Keep this category separate from the registration section. Name the channels clearly and make sure that saying no does not affect participation.

Reporting and evidence-related data

This may include attendance records, signatures, workshop feedback, or other limited data needed for project management, reporting, or audit duties.

Why we ask it:
We ask this data to show that the activity took place, to improve quality, and to meet project accountability requirements.

Instruction for youth workers:
Collect only what is necessary as evidence. Do not turn reporting into an excuse to keep every possible detail.

Why separate data categories?

Category	What it helps you do
Participation data	Run the activity.
Support data	Include and protect participants.
Emergency data	Act if something goes wrong.
Follow-up data	Stay in touch only if the person agrees.
Media data	Provide visibility only if the person chooses it.
Reporting data	Show what happened and what was achieved.

Remember: explain before you collect · collect less · separate purposes · limit access · delete with intention.

In your forms:

– Use clear sections for each category.

– Mark optional sections as optional.

– Provide a short purpose statement for each section.

– Avoid mixing optional permissions with necessary participation data.

– Review regularly and remove what you no longer need.

Sensitive data and support needs

Your turn -5 minutes

Open one form your organisation actually uses. Cross out every field you cannot justify in a single sentence. Move newsletter sign-up and photo permission into their own clearly optional boxes. That is it -you have just made your form more private and more trustworthy.

Youth projects sometimes need information about allergies, medication, access requirements, or mobility support. This can be necessary, especially when safety and inclusion are at stake. Still, good practice is to collect the minimum needed to support the person well. A youth worker rarely needs a full medical story. What the team usually needs is a short and relevant support instruction.

A safer way to ask

- Instead of asking for detailed medical history, ask what staff need to know to support safe participation. Always invite participants to bring their own, specific medications.

- Instead of asking broad open questions, use a short support-focused prompt such as: 'Please tell us only what is necessary for us to support your participation safely and respectfully.'

- Keep sensitive support notes separate from general attendance or dissemination records.

Minors' data

If minors are involved, the process needs extra clarity. Participation permission from a parent or guardian is not the same thing as optional permission for image use or newsletter communication. It is also not the same thing as your organisation’s safeguarding duties. The safest approach is to keep these functions separate, use plain language, and avoid forcing parents to agree to optional uses in order for the child to join the activity.

- Use a separate note for participation and safety information.

- Use a separate permission section for photos or videos where public use is planned.

- Make clear that refusing public-use permission will not affect participation.

- Check national rules if you plan to rely on a child's own online consent in any digital service context.

Chapter 3 checklist

- Have we removed fields that are interesting but not necessary?

- Is every optional use clearly separated from the participation process?

- Have we used plain language to explain the purpose before the form begins?

- If we collect support-related information, is access limited to the right people?

- If minors are involved, have we separated participation permission from optional privacy-related permissions?

Templates and worksheets

Template 3.1 - Data-minimised participant form blueprint

Purpose	Use when	Completed by

Build a clean form without mixing purposes.	When designing a registration, workshop sign-up, or local participant application form.	The project team member designing the form.

Section A - Necessary for participation	Full name; contact email; phone number if needed; organisation or school if relevant; age group if relevant; emergency contact; logistical details required for delivery
Section B - Optional support information	Accessibility adjustments; dietary needs; other support notes explained in a support-focused way
Section C - Optional follow-up contact	Newsletter sign-up; alumni contact; future project opportunities
Section D - Optional media permissions	Photo and video permissions for clearly named channels
Short purpose line	Tell participants in one or two sentences why each section exists

Use note: Use separate screens or clearly separated sections if your digital form allows it.

Template 3.2 - 'Purpose explained' script for forms

Purpose	Use when	Completed by
Give people a short, spoken or written explanation before they fill in the form.	At the start of workshops, trainings, local activities, or partner selection calls.	Any team member who introduces the form.

Before you start, here is why we ask for this information. We need some details to organise the activity, communicate with you, and provide support where needed. A few questions may be optional. Where something is optional, you can leave it blank or say no. We will also tell you who can access the information, how long we keep it, and how you can contact us if you have a question about your data.

Template 3.3 - Sensitive support information mini-form

Purpose	Use when	Completed by
Collect only the information needed for safe and inclusive participation.	When dietary, health, or accessibility information is genuinely needed.	Participant or parent/guardian where relevant.

Question prompt	Please tell us only what we need to know to support your safe and full participation.

Support need	[Short description]
What staff need to do	[Practical instruction only]
Who may need to know	[Trainer / facilitator / hosting team / first-aid contact only]
Review or delete date	[Date]

Use note: Avoid collecting diagnosis details unless the activity genuinely cannot be delivered safely without them.

Template 3.4 - GDPR-safe attendance sheet

Purpose	Use when	Completed by
Record attendance without over-collecting.	During workshops, meetings, and trainings where attendance evidence is needed.	Facilitator or admin staff.

Header	Activity name; date; place; organiser
Columns	Full name | Signature or tick | Organisation or city if needed
Do not include	Home address, ID number, medical notes, social media handle, or other unrelated data
Storage note	Move the sheet to the project file after the session and avoid leaving copies in open rooms

Template 3.5 - GDPR-safe feedback form

Purpose	Use when	Completed by
Collect useful feedback without prompting unnecessary personal data.	At the end of workshops and local activities.	Participants, anonymously where possible.

Suggested introduction:

This feedback form helps us improve the activity and understand learning results. Please avoid writing sensitive personal information unless it is truly necessary.

Suggested questions:

1. What was most useful for you today?
2. What could be improved?
3. Do you feel more confident about privacy and data protection after this session?
4. Would you like to receive optional follow-up learning opportunities from us? [Yes / No]

If yes: [Email]

Template 3.6 - Parent or guardian information note

Purpose	Use when	Completed by
Give a clear explanation when minors take part in an activity.	Before collecting a minor's data for participation.	The organising organisation.

Information for Parent or Guardian

Your child has been invited to take part in [activity name].

We will use basic participant information to organise the activity, communicate practical details, provide support where needed, and manage participation safely.

If we plan to take identifiable photos or videos for public communication, we will ask for separate permission. Saying no to public image use will not affect your child's participation.

If you have a question about your child's data, please contact:
[Email]
[Organisation]

Lesson page - Build a better registration form

Aim	Duration	Group size	Materials
Help staff spot unnecessary questions and redesign forms around clear purposes.	45 minutes	4 to 16 people	One real form from your organisation, pens, and two colours of sticky notes

Step-by-step flow

Step	Time	What to do
1	5 min	Ask participants to read the form silently and mark every field they think is clearly necessary.
2	10 min	Use one colour for fields that are necessary and another for fields that seem optional, unclear, or outdated.
3	10 min	Discuss each doubtful field using the question: “What would happen if we removed this field?”
4	10 min	Rebuild the form into sections: necessary participation data, support data, optional follow-up, optional media permissions.

5	10 min	End by rewriting the opening purpose statement in plain language.

Debrief questions

- Which fields were added by habit rather than by a clear present need?
- Where are we mixing optional permissions with necessary participation data?
- Did our revised form become easier to explain to a participant?

Chapter 4

Media, Communication, and Sharing with Partners

Why this matters in youth work

Youth projects often want to be visible, engaging, and well documented. That is understandable. Photos, short videos, testimonials, newsletters, websites, and social media all help tell the project story. At the same time, these are exactly the moments where people feel exposed if the process is unclear or too pushy. This chapter helps youth workers communicate responsibly, collect permissions in a fair way, and share participant information with partners only when it is necessary and controlled.

Did you know?

When you post on social media, you may be sharing more than a photo. Apps like TikTok can pull biometric data - faceprints and voiceprints -from the videos people upload, not just a name or email. That information can be used to identify someone, profile them, or be sold on.

The takeaway for youth projects: treat the platforms you use as part of your data story, and help young people see what they are really sharing.

By the end of this chapter, the reader should be able to:

- understand that participation in an activity does not automatically mean agreement to public visibility
- collect and use photo or video permissions in a more specific, fair, and transparent way
- separate public communication, internal documentation, and newsletter contact into different decisions
- explain image use and communication choices in plain language
- handle partner data sharing using a **need-to-know** approach
- identify safer and less risky ways to use shared drives, messaging apps, and digital collaboration tools
- respond more confidently when a participant wants to **withdraw image permission** or asks how their data is being shared

How this helps in practice

This chapter helps youth workers balance visibility and respect. It supports more ethical dissemination, safer communication habits, and more disciplined partner sharing. It is especially useful for projects that rely on social media, newsletters, photos, videos, or cross-border coordination.

What you need to know

- Participation in an activity does not automatically mean agreement to public visibility.
- Photo, video, newsletter, and partner-sharing decisions should be separated and explained clearly.
- A refusal to appear in communication materials should never affect participation.
- Partner sharing must follow a need-to-know principle and should use controlled channels.

Strong takeaway: good communication practice protects both dignity and trust. The easiest way to keep visibility ethical is to make it specific, optional, and easy to revisit later.

Legal anchor: GDPR Articles 5, 6, 12-14, 21; Erasmus+ Project Results Platform Terms of Use; European Commission guidance on valid consent

Photos and videos without pressure

Do	Avoid
Ask first, name the channels	Treating consent as automatic

Do	Avoid
Make saying no easy and free	Bundling photo consent with sign-up
Offer a no-photo zone or badge	Vague “forever, everywhere” wording
Tell people how to withdraw later	Ignoring a later request to remove

Visibility is part of many youth projects, but it should never feel like a condition of participation. Identifiable photos and videos can be highly personal. They may show where someone was, who they were with, or what community they belong to. The fair approach is to be specific about which channels are planned, explain that saying no is acceptable, and avoid vague blanket permissions that cover everything forever.

Good habits for image use

- Use separate permissions for internal documentation and public communication where possible.
- Name the channels clearly, such as project website, partner websites, social media, newsletters, or printed materials.
- Explain how a person can withdraw later.
- Offer practical alternatives such as no-photo seating zones, wristbands, badges, or standing outside the camera frame.

Mailing lists and newsletters

A person who registers for one workshop is not automatically agreeing to long-term promotional contact. If you want to keep sending updates, opportunities, or campaign messages, that should be a clearly optional step. The language should be simple and it should be easy to unsubscribe or opt out later (to choose not to participate or to choose to be excluded from some aspects).

- Do not pre-tick newsletter boxes.
- Do not hide the subscription inside a long paragraph of other conditions.
- Do not use a past participant list as a permanent mailing list without a clear lawful basis and honest explanation.

Sharing data with partners

Cross-border projects often require partners to exchange participant information. The key is to share only what the receiving partner needs for a clear task. A hosting partner may need names, travel times, rooming information, or access-related notes. It does not need every field from the original application form. A well-run sharing process identifies the purpose, the exact fields, the transfer method, the access limit, and the deletion point.

Before you share a file with a partner

- State the purpose in one sentence.
- Trim the sheet down to the exact fields needed.
- Choose a controlled transfer route, not an open chat attachment.
- Limit access to named roles or named people.
- Set a review or delete date after the practical need ends.

Using WhatsApp, shared drives, and digital tools

Most youth projects use fast digital tools because they are easy and familiar. The problem is not the existence of these tools. The problem is uncontrolled habits. A team chat should not become the permanent archive for registration exports, support notes, or passport copies. Shared drives should not stay open to everyone forever. The best approach is to use project-only spaces, keep access lists short, and clean them up after the activity.

- Avoid posting full participant lists in group chats.
- Do not send sensitive support information in open channels when a direct message or secured note would do.
- Use project-specific folders instead of personal accounts where possible.
- Review access after the activity and remove people who no longer need it.

Chapter 4 checklist

- Have we made public visibility genuinely optional?
- Do our permission forms name the channels rather than using vague blanket wording?
- Do participants know how they can change their mind later?
- Are we sending only the partner data that is actually needed for delivery?
- Are our project tools organised in a controlled way rather than through personal habits?

Templates and worksheets

Template 4.1 - Photo and video permission for adults

Purpose	Use when	Completed by
Collect a clear and channel-specific permission for identifiable image use.	Before taking or publishing identifiable photos or videos for optional visibility purposes.	Adult participant.

Photo and Video Permission

Activity:
Date:
Location:

Your choice below is optional. Saying no will not affect your participation.

I allow the organisers to use identifiable photos or videos of me for:
[ ] Internal documentation and Erasmus+ reporting
[ ] Project website
[ ] Partner websites
[ ] Social media
[ ] Newsletters or communication materials

I understand that I can later ask to withdraw this permission by contacting:
[Email]

Name:

Signature: Date:

Use note: If your project regularly needs only internal documentation, consider a separate and simpler internal-use option.

Template 4.2 - Photo and video permission for minors

Purpose	Use when	Completed by
Collect optional image permission in a child-sensitive and parent-facing format.	When minors are involved and public-use photography or video is planned.	Parent or legal guardian.

Photo and Video Permission for a Minor Child's name: Activity: Date: I am the parent or legal guardian of the child named above. I allow the organisers to use identifiable photos or videos of my child for: [ ] Internal documentation and Erasmus+ reporting [ ] Project website [ ] Partner websites [ ] Social media [ ] Newsletters or communication materials I understand that this permission is optional and that refusal will not affect my child's participation. I understand that I may later request withdrawal by contacting: [Email] Parent or guardian name: Signature: Date:

Template 4.3 - Withdrawal request for image use

Purpose	Use when	Completed by
Make it easy for a person to change their mind.	When someone wants to stop future use of their image or	Participant or parent/guardian.

	requests removal where reasonably possible.	

Subject: Withdrawal of photo or video permission

Hello,

I would like to withdraw permission for the use of my image, or the image of my child, in connection with [project or activity name].

Please stop using this material in new publications and remove existing content from your channels where reasonably possible.

Name:
Activity:
Date:
Contact details:

Template 4.4 - Newsletter sign-up wording

Purpose	Use when	Completed by
Collect a separate and simple opt-in for future communication.	In registration forms, exit forms, or local workshops.	Participant.

Would you like to receive occasional updates, learning materials, and future opportunities related to this project?

[ ] Yes, I would like to receive updates by email.

You can stop receiving these messages at any time.

Template 4.5 - Partner data-sharing note

Purpose	Use when	Completed by
Document what is being shared, why, and with whom.	Before sending participant information to a partner or service provider.	The person initiating the sharing.

Purpose of sharing	[Short one-sentence reason]
Receiving organisation	[Name of partner or provider]
Fields shared	[List exact fields only]
Why the recipient needs them	[Hosting / travel / support / reporting / other]

Transfer route	[Restricted folder / secure email / platform]
Access limit	[Named roles or named persons]
Review or delete date	[Date]
Responsible sender	[Name / role]

Use note: If a partner needs only a filtered list, do not send the full registration export. In case you have a partner from some of the third countries, please refer to the "**Working with non-EU partners**".

Template 4.6 - 'Before the group photo' script

Purpose	Use when	Completed by
Give participants a respectful reminder in the moment.	Before group photos, interviews, or video clips during live activities.	Facilitator, MC, or communication lead.
We would like to take some photos or short video clips for project communication. This is optional. If you do not want to appear, please let us know now or move to the no-photo area. Saying no will not affect your participation in any way.		

Lesson page - Visibility without pressure

Aim	Duration	Group size	Materials
Help a team plan communication that respects participant choice.	40 minutes	5 to 20 people	Flipchart, marker, sample project communication channels

Step-by-step flow

Step	Time	What to do
1	5 min	List all communication channels the project wants to use, such as website, Instagram, Facebook, newsletter, and final report.
2	10 min	Ask the group which channels are essential and which are simply nice to have.
3	10 min	Design a fair permission flow that separates internal documentation, public communication, and optional newsletter contact.
4	10 min	Discuss practical inclusion measures such as no-photo zones, alternative shots, back-of-group images, and scene photos without identifiable faces.
5	5 min	End by drafting the one-sentence explanation the team will use before photos are taken.
Debrief questions		

- Where do participants feel most pressure to say yes?
- Could our visibility goals still be met with less intrusive content?
- Are we prepared to act quickly if someone later asks us to stop using their image?

Chapter 5

Storage, Security, and Retention

Why this matters in youth work

The moment a form closes or a workshop ends, privacy work does not stop. Files need to be stored, access needs to be reviewed, and temporary copies need to disappear. This is where small NGOs often struggle, not because they lack goodwill, but because folders grow, staff change, and nobody makes time for clean-up. This chapter turns storage, security, and deletion into manageable routines that youth workers can actually follow.

By the end of this chapter, the reader should be able to:

- identify where project data is officially stored and where duplicate or uncontrolled copies may exist
- apply simple but effective **security habits** suitable for small NGOs and youth teams
- limit access to personal data based on real roles and tasks
- understand the difference between keeping records for valid reporting or audit reasons and keeping data without a clear purpose
- create or follow a **retention schedule** for different types of project records
- carry out a basic folder and access clean-up after an activity
- respond more calmly and systematically if a small privacy incident happens

How this helps in practice

This chapter helps youth workers move from vague intentions to concrete routines. It is especially useful after activities, when files, attendance sheets, exports, support notes, and photos often remain scattered across devices and folders. It helps teams store data in a more disciplined way, reduce unnecessary access, and delete information when it is no longer needed.

What you need to know

- Good privacy protection often depends on small consistent habits rather than expensive systems.
- Access should follow roles and practical need, not broad curiosity or convenience.
- Sensitive support information should be stored separately from ordinary participant records where possible.
- Retention means deciding what must be kept, what should be reviewed, and what should be deleted.

Strong takeaway: security is not only about stopping a breach. It is also about preventing drift, where too many files, too many copies, and too many people keep access longer than they should.

Legal anchor: GDPR Articles 5 and 32; Erasmus+ Programme Guide Part C on record retention and checks; ENISA cybersecurity guidance for SMEs

Where data is stored

Small organisations often store data in several places at once. A registration export may sit in the form tool, in a coordinator's downloads folder, in a shared drive, and in an old email attachment. That makes deletion difficult and increases the chance of accidental exposure. A healthier system is to decide one main storage location for each process, limit duplicates, and remove local copies once the official version is safely stored.

A good storage map answers four things

- What type of data is stored here?
- Who can access it?
- Why is this the official location?
- When will it be reviewed or deleted?

Practical security for small youth NGOs

A youth organisation does not need enterprise-level infrastructure to improve data security. It does need discipline. Strong passwords, multi-factor authentication, device locks, project-specific folders, and clean access lists already make a major difference. The aim is not perfection. The aim is to reduce predictable risks that happen when teams work fast and nobody checks the basics.

- Use unique accounts wherever possible.
- Enable multi-factor authentication on the main project tools.
- Avoid sharing whole folder trees with wide groups if only two people need access.
- Do not keep participant files on personal devices longer than necessary.
- Review shared links and guest permissions after each major activity.

Retention schedules and deletion routines

Retention is often misunderstood. It does not mean deleting everything immediately, and it does not mean keeping everything forever. The point is to match the retention period to the real purpose. Some project records may need to be kept to meet audit or reporting duties. Other information, especially support-related notes or duplicate exports, should go much sooner. A simple retention schedule keeps this balanced and defensible.

> A practical rule for Erasmus+ records
>
> For grants not exceeding EUR 60.000, the Erasmus+ Programme Guide states that records, supporting documents, statistical records, and other grant-related documents may need to be kept for up to three years after final payment. This does not justify keeping every participant detail in every location. It means you should identify what truly counts as supporting evidence and store it in a controlled way.

Incident readiness

Even in small projects, things can go wrong. A laptop may be lost. A file may be shared with the wrong person. A participant list may be left open on a projector. The most useful response is calm, documented, and practical. Note what happened, what data was involved, who was affected, what you did immediately, and what will change next time.

- Contain the issue quickly.
- Record the facts without panic or blame.
- Inform the right internal person immediately.
- Review whether further notification is needed under your organisation's process or legal advice.

Chapter 5 checklist

- Do we know the official storage location for each key project process?
- Have we reduced duplicate files and local copies?
- Is access limited to people who genuinely need it?
- Do we have a simple retention schedule rather than vague intentions?
- Can our team document and review a privacy incident if one happens?

Templates and worksheets

Template 5.1 - Access control and storage checklist

Purpose	Use when	Completed by

Map official storage points and reduce uncontrolled access.	At project start, before large activities, and during periodic clean-up.	Coordinator, admin lead, or digital tools lead.

Process	[Registrations / support notes / photos / partner sharing / reporting]
Official storage location	[Folder or platform]
Who has access	[Named roles or named people]
Why they have access	[Task-based reason]
Sensitive data stored separately	[Yes / No / Not applicable]
MFA enabled	[Yes / No]
Review date	[Date]

Template 5.2 - Retention schedule template

Purpose	Use when	Completed by
Define what should be kept, for how long, and why.	At the beginning of the project and after major activity cycles.	Coordinator together with the person managing records.

Data or document type	[Registration list / attendance sheet / photo permission / support note / newsletter list / financial evidence]
Purpose	[Delivery / support / reporting / audit / communication]
Access limit	[Roles only]
Keep until	[Date or event]
Delete or anonymise on	[Date]
Why this period is justified	[Short reason]

Use note: Keep the schedule realistic. A schedule nobody follows is not a useful one.

Template 5.3 - Before, during, and after activity checklist

Purpose	Use when	Completed by
Turn good privacy habits into a practical routine.	For trainings, workshops, exchanges, and local events.	Activity lead or assigned privacy focal point.

Before	Review the form; remove extra fields; prepare the privacy notice; set the official folder; test who has access

During	Keep paper lists secure; avoid open sharing of support details; remind the team about photo choices; use approved tools only
After	Move files to the official folder; delete duplicate local copies; review access; delete temporary support notes where appropriate; update the retention log

Template 5.4 - Data incident log

Purpose	Use when	Completed by
Record what happened and what the team did in response.	Whenever an accidental disclosure, loss, or other privacy incident occurs.	The person designated to log incidents.

Date and time	[DD/MM/YYYY HH:MM]
What happened	[Short factual description]
Data involved	[Type of data]
People potentially affected	[Number or group]
Immediate containment step	[What was done first]
Who was informed internally	[Name / role]
Follow-up action	[Access changed / files deleted / staff briefed / other]
Closed on	[Date]

Template 5.5 - After-project clean-up worksheet

Purpose	Use when	Completed by
Help the team close the project without leaving personal data scattered.	At the end of the project or after a major reporting milestone.	Coordinator with admin support.

Old guest access removed	[Yes / No]
Duplicate participant exports deleted	[Yes / No]
Sensitive temporary notes removed	[Yes / No]
Open shared links reviewed	[Yes / No]
Remaining records matched to retention schedule	[Yes / No]
Responsible person	[Name]

Date completed	[Date]

Lesson page - The 20-minute folder reset

Aim	Duration	Group size	Materials
Give staff a repeatable mini-routine for storage and access clean-up.	20 to 30 minutes	2 to 8 people	Laptop access to the project folder structure and one printed clean-up worksheet

Step-by-step flow

Step	Time	What to do
1	5 min	Open the main project storage space and identify which folder is the official source for registrations, support notes, photos, and reporting files.
2	5 min	Check who currently has access and remove any clearly outdated or unnecessary permissions.
3	5 min	Find duplicate local copies, old exports, and temporary files that no longer have a reason to stay.
4	5 min	Update the retention schedule for anything that must be kept longer.
5	5 min	Record what was removed, what was kept, and what still needs follow-up.

Debrief questions

- Which files stayed only because nobody took ownership of deletion?
- Where do we still rely on personal laptops or old email threads instead of official storage?
- Which access rights would surprise a participant if they saw them today?

Lessons support

Lesson - Who decides what?

Print and cut these cards before the session. Give one card to each small group, or mix them and let groups rotate after a few minutes. Ask participants to decide who decides the purpose, who only handles data on someone else's behalf, and who should answer participant questions.

Use tip: Do not reveal the answer key immediately. Let the groups explain their reasoning first.

Scenario Card 1 - Registration form for a training course
Situation
The lead partner creates one online registration form for all youth workers joining a transnational training course. It decides which questions to ask, when the deadline is, and how the information will be used. The other partners only send the form link to their own participants and encourage them to complete it.
Group task
Who decides the purpose of this data collection?
Are the other partners also controllers for this form, or are they only helping with outreach?
Who should answer if a participant asks to access or correct their data?
Facilitator answer
Most likely, the lead partner is the controller for this form. The other partners may be separate controllers for their own local selection process, but not automatically for the shared form. If the partners jointly agreed on the form fields and purpose, then this may become a joint-controller situation and should be documented clearly.

Scenario Card 2 - Hotel rooming list and dietary details
Situation
The hosting partner needs to book accommodation and meals for participants. It asks the other partners to send names, arrival times, room-sharing preferences, dietary needs, and accessibility requirements in one shared spreadsheet.
Group task
Which data is really necessary for the booking process?
Who is the controller for the hotel and meal arrangement process?
Should all partners have access to dietary and accessibility details?
Facilitator answer
The hosting partner is usually the controller for the accommodation and meal process because it decides why that data is needed. Other partners should share only what is necessary. Sensitive information, such as dietary, health, or accessibility details, should have restricted access and should not sit in a folder visible to everyone.

Scenario Card 3 - Newsletter sign-up after the project
Situation
After the activity, one partner wants to keep all participant email addresses and add them to its organisation's newsletter list so it can share future opportunities and local events.
Group task
Can the partner use the same participant list for a newsletter?
Is this still part of the original participation purpose?
What should the partner do before adding people to the mailing list?
Facilitator answer
No, the partner should not automatically reuse the participant list for a newsletter. Future promotional communication is a different purpose. In most youth-work situations, the safest approach is a separate optional sign-up with clear information and an easy way to withdraw or unsubscribe.

Scenario Card 4 - Photos for Instagram and partner websites
Situation

During a youth exchange, the Serbian partner takes many photos and short video clips. After the activity, all partners want to use the same material on their own websites, social media pages, and newsletters.
Group task
Is participation in the activity enough to publish identifiable photos?
Who is responsible when each partner publishes the same photo on its own channels?
How should the team handle a later request to remove an image?
Facilitator answer
Participation alone is not enough for public image use. If the person is identifiable, the team should rely on a clear and specific permission process or another appropriate legal basis. Each partner publishing on its own channels acts as controller for that publication. The partnership should agree in advance how withdrawal or removal requests will be handled.

Scenario Card 5 - Shared Google Drive folder for all partner staff
Situation
To keep everything in one place, the coordinator creates a shared cloud folder with registration data, travel details, emergency contacts, and health-related support notes. All partner staff receive full access because it seems practical.
Group task
What is useful about this arrangement and what is risky?
Which data should not be visible to every staff member?
What simple access-control changes would improve this process?
Facilitator answer
A shared folder may be practical, but full access for everyone is not good practice. Sensitive support notes and health-related information should be in a separate restricted area. Access should be role-based, not general. Staff should only see what they need to do their job.

Scenario Card 6 - External company prepares certificates
Situation
The Cypriot partner hires an external service provider to generate certificates from a participant list. The company receives names, organisations, and attendance data, follows the partner's instructions, and sends the final files back.
Group task
Is the external company deciding the purpose of the data use?
Is it more likely to be a controller or a processor?
What should the youth organisation have in place before sending the list?
Facilitator answer
This is usually a processor situation. The youth organisation still decides why the data is used, and the external company only acts on instruction. Before sharing the list, the organisation should make sure there is a proper processing arrangement, clear instructions, limited data sharing, and secure transfer.

Scenario Card 7 - Injury note posted in a WhatsApp group
Situation
During an outdoor activity, a participant has a medical issue. A volunteer writes the participant's name, symptoms, and medication details in a large WhatsApp group that includes all partner staff, some volunteers, and one external photographer.
Group task
What went wrong here?
Who really needed this information?
How should the team record and share incident information instead?
Facilitator answer

The main problem is unnecessary disclosure. Sensitive information was shared too widely in an informal channel. The team should move to a controlled incident process, limit access to the people who need to act, and record only the information necessary for safety, follow-up, and accountability.

Scenario Card 8 - Uploading project outputs to the Erasmus+ platform Situation The coordinator wants to upload a handbook and a short dissemination video to the Erasmus+ Project Results Platform. The video includes participant faces, names on workshop flipcharts, and short interview clips. Group task What should the coordinator check before uploading? Is every visible piece of personal data necessary in the final version? Who inside the partnership should approve publication of the final material? Facilitator answer Before upload, the coordinator should check whether the material includes personal data, whether that personal data is really necessary, and whether the partnership has the right permissions or another valid basis for publication. The safest approach is to minimise identifiable content, confirm permissions, and use a clear internal approval step before publication.

Lesson - The 20-minute folder reset

Support sheet - Printed clean-up worksheet

Use this page during the activity. Print one copy for the team, or complete it together on screen while you review the project folders.

Project or activity	[Name]
Date of reset	[DD/MM/YYYY]
People completing the reset	[Names / roles]
Main project storage space reviewed	[Drive / folder / platform]

Part A - What is the official source?

Registrations	[Official folder or system]
Support notes	[Official folder or system]
Photos and videos	[Official folder or system]
Reporting files	[Official folder or system]
Partner sharing files	[Official folder or system]

Part B - What did we clean up?

Item to review	Status	Notes
Old guest access removed	[Yes / No / Partly]	[What changed?]

Duplicate participant exports deleted	[Yes / No / Partly]	[Where were they found?]
Temporary support notes removed	[Yes / No / Partly]	[What was deleted?]
Open shared links reviewed	[Yes / No / Partly]	[Which links still remain open?]
Outdated files moved or deleted	[Yes / No / Partly]	[Which folders need more work?]

Part C - What must still be kept?

Record or file set	Why it is still needed	Keep until / owner
[Example: attendance evidence]	[Reporting / audit / follow-up]	[Date / name]
[Example: photo permissions]	[Evidence of permission]	[Date / name]
[Add item]	[Reason]	[Date / name]
[Add item]	[Reason]	[Date / name]

Part D - Sign-off

Person responsible for follow-up	[Name / role]
Next review date	[DD/MM/YYYY]
Biggest risk we noticed today	[Short note]
One action we will complete this week	[Short note]

Chapter 6
Incidents, Breaches & Quick Response

Why this matters in youth work

Even careful teams make mistakes. A registration list sent to the wrong address, a shared link that stayed open too long, a laptop left on a train, a screenshot shared in a public chat. These are the privacy incidents that youth organisations actually face. This chapter does not assume your team will be perfect. It gives you practical tools to respond quickly, document clearly, and learn from what went wrong. Knowing what to do in the first hour makes the difference between a managed setback and a damaging situation.

What you need to know

- A privacy incident is not the same as a reportable breach. Most incidents can be managed internally without formal notification to a supervisory authority.
- The first hour matters most. A calm and documented response is far better than a delayed or panicked one.
- You do not need to solve everything at once. Contain the situation, document what you know, and then decide what comes next.
- Transparency with affected participants, where appropriate, rebuilds trust faster than silence.

Typical risk scenarios

Understanding the most common incidents in youth work helps your team prepare before something happens. These are the situations organisations encounter most often:

- Wrong email: A registration list, support note, or participant file is sent to the wrong person or group by mistake.

- Open shared link: A file containing participant data is shared via a link that is set to public instead of restricted. Anyone with the link can access it.

- Lost or stolen device: A phone, laptop, or USB drive containing project data is lost or taken. This is especially serious if the device is unencrypted or unlocked.

- Unprotected file: A spreadsheet of participant names or contact details is saved locally on a personal computer without a password, or uploaded to a personal cloud account.

- Accidental publication: A photo, document, or list that was not meant to be public is posted to social media or a project website.

- Insider access: A volunteer or temporary staff member accesses participant data they did not need to see for their task.

What to do in the first 24 hours

The moment you discover a privacy incident, the same basic steps apply regardless of the type or scale of the problem.

- Step 1 - Contain: Stop the situation from getting worse. Remove the open link, recall the email if possible, lock or remotely wipe the device, or take down the accidental publication.

- Step 2 - Identify: List what data was involved, who might have been affected, and how the incident happened.

- Step 3 - Record: Open your incident log immediately and write down what you know. Do not wait until the situation is resolved.

- Step 4 - Inform internally: Tell the responsible person in your organisation. Do not manage a significant incident alone.

- Step 5 - Assess: Decide whether the incident is likely to result in a risk to the rights and freedoms of the people affected. If yes, or if you are unsure, seek advice.

- Step 6 - Communicate if appropriate: If participants are at real risk, inform them clearly and promptly. Explain what happened, what you have done, and what they can do to protect themselves.

Documentation and communication basics

Your incident log is the most important tool in any privacy incident. It does not need to be complex. It needs to be accurate, factual, and completed as quickly as possible after the incident is discovered. A good log entry includes the date and time, what happened, what data was involved, who may have been affected, what steps were taken immediately, who was informed and when, and what will change to prevent a recurrence.

When communicating with affected participants, keep the message short, honest, and practical. Explain what you know without speculation. Tell them what you have done. Give them a contact they can use. Avoid technical or legal language. The goal is to be helpful, not to manage reputation.

When to escalate or seek advice

Not every incident needs to go beyond your internal team. You should escalate or seek external advice when: the incident involves sensitive data such as health information, financial details, or identity documents; a significant number of participants may be affected; there is reason to believe the breach was deliberate; you cannot determine what data was involved or who accessed it; or participants are likely to face real consequences as a result of the incident.

Under GDPR, certain breaches must be reported to the relevant supervisory authority within 72 hours of becoming aware of them. This requirement applies when the breach is likely to result in a risk to the rights and freedoms of individuals. If in doubt, check with your organisation's leadership or seek specific data protection advice before the 72-hour window closes.

Chapter 6 checklist

- Does your team know who to contact first if a privacy incident is discovered?
- Is there an incident log template ready to use before an incident happens?
- Have you practised a short scenario exercise with your team so they know the first steps?
- Do you know when your organisation is required to report internally and when to seek external advice?

Templates and worksheets

Template 6.1 - Incident assessment and log

Purpose: Record what happened, assess the risk, and track your response.

Use when: Immediately after discovering a potential or confirmed privacy incident.

Completed by: The person who discovers the incident, then reviewed by the named privacy contact.

Incident ID: [Internal reference number]

Date and time discovered: [DD/MM/YYYY and time]

Discovered by: [Name and role]

Description of what happened: [Brief factual account]

Data involved: [Types of data and estimated number of records]

Who may be affected: [Participants / staff / partners]

Immediate containment action taken: [What you did first to stop the situation worsening]

Internal person notified: [Name / role / date and time]

Risk level assessment: [Low / Medium / High -and why]

Communication to participants needed: [Yes / No / Under review]

Further action required: [Short list of next steps]

Incident closed on: [DD/MM/YYYY]

What will change: [Concrete measure to prevent recurrence]

Use note: Keep the log factual and neutral. Do not include speculation, blame, or legal conclusions without professional advice.

Template 6.2 - Participant communication after an incident

Purpose: Inform affected participants clearly and calmly when they need to be told.

Use when: When the assessment indicates that participants face a real risk from the incident.

Completed by: The project coordinator or privacy contact, reviewed before sending.

Lesson page - What would you do? Incident response practice

Aim Duration Group size Materials

Build practical confidence in responding to privacy incidents quickly and calmly. 40 minutes 4 to 20 people Scenario cards (one per group), incident log template, and this chapter

Step-by-step flow

1 5 min Introduce the three most common incident types in youth work: wrong email, open shared link, and lost device. Ask participants which they have seen or worried about.

2 15 min Divide into groups of three. Each group receives one scenario card describing an incident. They have five minutes to decide: what do you do first, who do you tell, and what do you write in the log?

3 10 min Groups present their decisions. Facilitator highlights what was right, what was missed, and what the 24-hour steps would look like in each case.

4 5 min Agree as a full group: who is our first contact if an incident happens? Do we know where the incident log template is? What would we do differently from today?

5 5 min Close by reminding the group that a calm and documented response to a small incident is far better than a panicked and delayed one.

Debrief questions

- Which scenario felt most realistic for our team?
- Were there steps we would not have thought of without this exercise?
- Is our team prepared to respond if something happened this week?

Key message: A fast and honest response to a small incident is always better than a slow or hidden one.

Chapter 7
For Young People: Protect Your Data Online

This part of the toolkit is written for you -the young people taking part in projects, workshops, and exchanges. The rest of the handbook helps the adults run things safely. This chapter is about your data, your rights, and a few easy habits that keep you in control online.

Your data is worth more than you think

Every time you sign up, post, scroll, or let an app 'access' something, you leave a trail. That trail is valuable. Companies use it to build a profile of who you are, what you like, and what you might buy or believe. Most of this happens quietly, in the background, in settings you never opened.

What your favourite apps can collect about you

Your location	Your contacts
Photos and faceprints	Your voice
What you watch	Who you message
Browsing history	Device and IP address

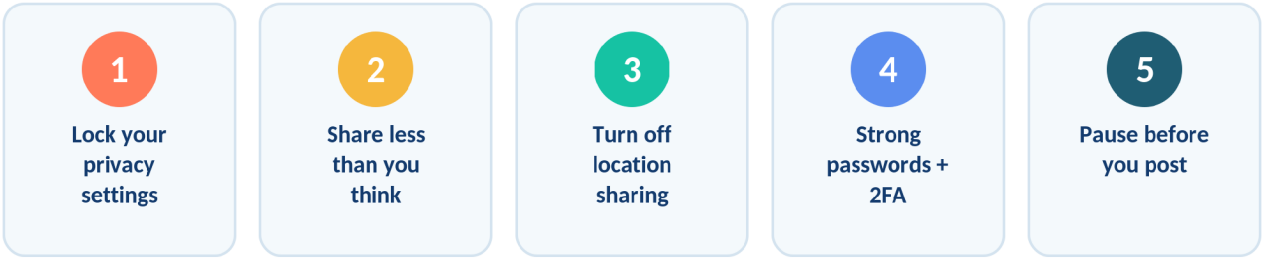
The point is not to scare you -it is to help you choose what you share.

Did you know?

Apps like TikTok can collect biometric data -your faceprint and voiceprint -from the videos you upload, not just your name or email. That data can be used to identify you, target you, or be sold on. You cannot always undo it, so the smartest move is to share a little less in the first place.

Five smart habits

Five smart habits to protect your data online



- Lock down your privacy settings. Set new accounts to private and check who can see, comment, and message you.
- Share less than you feel like sharing. Location tags, your school, your daily routine, and your full birthday are easy for strangers to misuse.
- Turn off location sharing for apps that do not truly need it. A photo filter does not need to know where you sleep.
- Use strong, different passwords and turn on two-factor authentication. One leaked password should not unlock your whole life.
- Pause before you post. Ask yourself: would I be okay with this in five years, seen by a teacher, an employer, or a stranger?

Know your rights

Data protection law (the GDPR) gives you real rights over your personal data -and you can use them as a young person too.

- See it: ask a company or organisation what data they hold about you.
- Fix it: ask them to correct anything that is wrong.
- Delete it: in many cases you can ask them to erase it.
- Say no: refuse or withdraw permission for optional things, like marketing or having your photo published.
- Complain: if an organisation mishandles your data, you can contact your national data protection authority.

If something goes wrong

Mistakes, leaks, and unkind behaviour happen online. If something feels wrong -an account is hacked, an image is shared without your consent, someone is threatening or impersonating you -here is what to do.

What to do

Do not panic, and do not blame yourself.
Save the evidence: screenshot the messages, links, and usernames with the date before anything is deleted.
Report and block inside the app, and change your password.
Tell someone you trust -a youth worker, teacher, parent, or friend. You do not have to handle it alone.
For serious cases (threats, identity theft, intimate images, or anything involving a minor), contact the platform's safety team and, if needed, the police or a national helpline.

Your 60-second privacy check

Are my main accounts set to private?
Is two-factor authentication on for my email and socials?
Have I turned off location for apps that do not need it?
Do I know how to report and block?
Is there one adult I would tell if something went wrong?

Trainer's Guide: Running Sessions with Young People

This chapter is for youth workers and trainers who want to run sessions with young people on data protection and online safety. It builds on the 'For Young People' chapter and supports the project's train-the-trainers and local-workshop activities. You do not need to be a legal expert -you need to make the topic relatable, active, and judgement-free.

Principles for sessions with young people

- Make it relatable, not preachy. Start from the apps and situations they actually use.
- Keep it active. Short inputs, then discussion, challenges, and decisions -not lectures.
- Create a safe space. No shaming anyone for what they have shared; everyone is learning.
- Use real examples, not fear. The goal is confident choices, not anxiety.
- End with action. Every participant should leave with one concrete change they will make.

A ready-to-run 90-minute workshop

At a glance

Aim: build practical confidence in protecting personal data online
Audience: young people, roughly 13 to 25
Duration: 90 minutes
Group size: 8 to 25
Materials: this chapter, the 'For Young People' pages, sticky notes, phones (optional), flipchart

- (10 min) Welcome and warm-up. Quick poll: 'How many apps asked you for permission this week?' Agree ground rules: no judgement.
- (20 min) What do apps know? In small groups, list everything one favourite app might collect, then reveal with the 'What your apps can collect' graphic and discuss the surprises.
- (20 min) Privacy-settings challenge. In pairs, open one account's privacy settings and find three things to change. Share the best find with the room.
- (20 min) Your rights and what to do. Walk through the five rights and the 'if something goes wrong' steps using a real scenario, such as a leaked photo or a hacked account.
- (15 min) Commitments. Each person writes one habit they will start this week; volunteers share.
- (5 min) Close and feedback. Capture learning with the feedback form (Template 3.5).

Three activities you can drop in

- Spot the oversharing (10 min): show a mock profile or post; groups identify what reveals too much, and why.
- Permission audit (10 min): participants review the app permissions on their own phone and switch off two they do not need.
- Rights role-play (15 min): one participant 'asks' an organisation to delete their data while another plays the organisation; debrief what a good response looks like.

Adapting for age and setting

- Younger groups (under 15): focus on settings, location, and telling a trusted adult; keep examples concrete.
- Older groups (16+): add rights, consent, and the data-economy angle -how data is profiled and sold.
- Online delivery: use polls and breakout rooms, and never ask participants to show real personal accounts on screen.

Facilitator tips

Keep phones as a tool, not a distraction. Protect privacy in the room -no one has to reveal their real accounts. Close on empowerment, not fear. And use Template 3.5 to capture feedback so each session gets better.

Appendix

Ten working principles to keep beside your desk

- If you do not need it, do not collect it.
- If it is optional, say so clearly.
- If it is sensitive, collect less and protect more.
- If you share it, be able to explain why.
- If you publish it, make sure the person has a real choice.
- If minors are involved, separate participation, safeguarding, and optional permissions.
- If several partners are involved, write down who is responsible for what.
- If a participant asks a question, answer through a clear and respectful route.
- If the activity is over, review what can be deleted now.
- If your team cannot explain the process simply, the process still needs work.

Selected legal and practice references used to build this toolkit

The toolkit is grounded in practical privacy principles from EU data protection law and Erasmus+ implementation guidance. The sources below are useful if you want to check the legal background, adapt a template more formally, or brief your organisation's leadership team.

- Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)
- Regulation (EU) 2018/1725 - data protection for EU institutions, bodies, offices, and agencies
- European Commission guidance on GDPR principles, information duties, data minimisation, sensitive data, and valid consent
- European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- Erasmus+ Programme Guide, Part C and 'Other important provisions', including record retention and data protection sections
- Erasmus+ Project Results Platform Terms of Use
- ENISA guidance for SMEs on basic cybersecurity practices
- SALTO-YOUTH resources on digital youth work, data storage and security, and practical digital safety methods

Good practices from the field

These short principles distil the most common lessons from real youth projects. Use them as a quick reference, or as discussion prompts with your team.

- Ask for less. Every field you remove is a risk you remove.
- Separate the optional from the required, always -especially photos and newsletters.
- Name one privacy contact per project, and put it on every form.
- Share filtered lists with partners, never the full export.
- Keep sensitive support notes in a separate, restricted place.
- Agree roles in writing before the first registration opens.
- Review access and delete duplicates after every activity.
- Treat a small incident seriously and calmly -document it the same hour.

Further resources and links

These trusted sources are useful if you want to go deeper, brief your leadership, or adapt a template more formally.

- GDPR (Regulation (EU) 2016/679) -the full legal text, via EUR-Lex.
- European Data Protection Board (EDPB) -official guidelines, including on controller and processor concepts.

- European Commission -plain-language guidance on data protection rules and your rights.
- Erasmus+ Programme Guide, Part C -record-keeping, retention, and data protection for projects.
- ENISA -basic cybersecurity guidance for small organisations.
- SALTO-YOUTH -practical resources on digital youth work and online safety.
- Better Internet for Kids and national Safer Internet Centres -youth-facing online-safety resources and helplines.
- Your national Data Protection Authority -for rights questions and complaints.

How to adapt these templates well

- Replace bracketed placeholders with your real organisation details.
- Do not copy optional permission text into mandatory participation sections.
- Adjust retention periods to your actual grant and record-keeping obligations.
- If you face a complex case, such as a major incident or a dispute about a data subject request, seek specific legal or data protection advice.