realife Learning - Data Protection & Ethical Data Practice workshop script

About this training

This is a facilitator script for realife's data protection and ethical data practice training, written for a realife team member who is a data protection specialist to deliver online or in-person to staff, associates, or contracted consultants. It is not designed for delivery by someone without the specialist knowledge and background. It can be provided after the session to staff members for reference along with the recording of the session.

The session uses roleplay as its primary method. You move between three characters: a South African activist whose data realife has collected; a colleague at a partner organisation; and a freelance facilitator being contracted by realife. Participants play themselves throughout.

It needs to be delivered yearly - and at the start of a new project. All training is logged.

Adapt it to the specific roles of those involved in the session (for example some areas can be left out entirely such as specific research methods and others may be given more time). Inline facilitator notes flag where to adjust examples for the specific project context, role type, or geography of the group.

This training presumes a pre-existing level of sensitivity to ethical considerations which can be both trained in academic backgrounds of many realife colleagues but also in how people without academic backgrounds have experienced working in communities with sensitivity to keep people safe. If during recruitment this is identified as an areas lacking then additional training may be required.

The three characters:

The activist: a South African political activist and community organiser, recently interviewed by realife for an evaluation project. Politically aware, not easily reassured, warm but not deferential. Note - the same would apply for any contact of realife: a partner organisation, a learner, a colleague.

The partner colleague/me: They contact realife via message in various scenarios. Read their messages aloud and respond as yourself.

The freelance facilitator: contracted by realife to deliver a Learning Landscapes session. Experienced, enthusiastic, asking practical questions.

Timing overview - flexible to meet needs and focus

Section	Content	Character	Time
1	Welcome and framing	Yourself	5 min

2	Character introduction + why collect data	The activist	10 min
3	Sensitive data and consent	The activist	10 min
4	Survey design, platforms, and data storage	Colleague interlude	7 min
5	Anonymisation and identity protection	The activist	12 min
6	AI tools, storage, and security	The activist	8 min
7	Photography, video, and children	The activist + interlude	10 min
8	Sharing data and partner organisations	The activist + colleague	10 min
9	Secondary data and cross-border transfers	Colleague interlude	8 min
10	Access requests and deletion	The activist	10 min
11	Breach response — yours	Colleague-to-colleague	10 min
12	Breach response — a partner's	Colleague message	8 min
13	The contracted facilitator	The freelance facilitator	10 min
14	Outcome Harvesting and MSC	Colleague interlude	7 min
15	Retention schedules	Colleague-to-colleague	5 min

16	Ethics beyond compliance	Yourself	10 min
17	Close and next steps	Yourself	5 min

SECTION 1 — Welcome and framing (5 min)

As yourself.

For this session I am not going to play the role of a data protection lead reading you legislation. No slides. No reading through legal frameworks - but they will come up.

Instead I'm going to move between three different characters across the next two hours — someone whose data realife has collected, a colleague at a partner organisation, and a freelance facilitator we're contracting. You play yourselves throughout.

No wrong answers - they will be the most generative - and if you want to throw in wrong answers on purpose then please do. This is not a test. Talk to each other - not just back and forth with me. That's where the learning happens.

I'll step out of character occasionally to link what we're discussing to the legal frameworks. Stop me at any point. The law matters! But this session is really about ethics, practice, and what it means to do this work the way realife believes in.

One framing note: POPIA in South Africa and GDPR in the UK are more similar than different in their core requirements. Where they diverge I'll name it. Follow good practice and you can meet both.

SECTION 2 — The activist: introduction and first question (10 min)

Hello. I live in South Africa. I'm not going to tell you exactly where, for reasons that will become obvious.

I was recently interviewed by someone from realife. We spoke on Zoom. Before that we had a few emails arranging the call. You said you wanted to talk about my activism. I've been involved in community organising and land rights work for about twelve years.

In the call I talked a lot. I told you my name. I talked about my family. I mentioned some health problems — I felt they were relevant, the stress of this work takes a toll. I talked about my political work, the organisations I'm involved with, some of the tactics we use. And I told you about the time I was arrested. Not convicted but I was arrested.

You recorded the call and used something called Otter AI to transcribe it automatically. I could also see you writing notes. Afterwards you sent me a short survey.

At the very start you explained what the project was about and what you'd do with everything I said. I was nervous. I can't really remember what you told me.

So first question for you to all consider.

QUESTION 1: For what purposes might it be acceptable for an organisation like realife to collect and record all of this about me?

Open to group discussion. 4–5 minutes.

Facilitator note: The core principle is purpose limitation: data must be collected for a clear legitimate purpose, must be necessary for that purpose, and cannot be repurposed without fresh consent. It has to be clearly for our interest or theirs — for ethical research purposes it always has to be for their interest. If we collect it and do nothing with it, we shouldn't have collected it. Name the real purposes relevant to this group's actual work.

If discussion stalls: "Imagine I told you all of that — and then nothing. The project was cancelled, the report never happened, and my interview is still sitting on your Google Drive. Is that acceptable? Is there anything else more important than respecting the dignity and safety of that person?"

SECTION 3 — Sensitive data and consent (10 min)

Still in character.

I want to say something. I shared a lot of personal things. And I shared them because they felt relevant. My health struggles are directly connected to the stress of this work. My arrest is part of my political history. I trusted you needed to know.

QUESTION 2: Is there anything I've told you that you'd consider particularly sensitive? Does it change how you handle it?

3–4 minutes. Draw out: health, arrest record, political views, family, organisational affiliations.

Facilitator note: GDPR has an explicit special category covering health data, political opinions, racial and ethnic origin, religious beliefs, biometric data, and trade union membership — these require additional legal justification to process. POPIA doesn't use the same tiered structure. In realife's practice we treat all personal data as sensitive, given the communities we work with.

Now — about consent.

I said at the start I was happy for realife to use what I said to write your report. I hope it helps the cause. You also mentioned sharing the recording with a local partner — I said I was fine with that, I trust them.

But do I need to sign anything? What exactly did I agree to?

QUESTION 3: What does proper consent look like — and what are your obligations?

4–5 minutes.

Facilitator note: Consent must be explicit, informed, and specific to stated purposes. Verbal consent is valid but must be captured as part of the raw data. Consent can be withdrawn at any time — participants may not know this right and we should tell them and should be prompted at the start and end of interviews. Consent given for one purpose doesn't automatically extend to others: a report is not a conference presentation is not a funding case study. Each new use needs checking. Children and vulnerable adults: consent for children usually requires a parent or guardian but the child's own views must be taken seriously. Coercive dynamics are often invisible, someone may feel they can't decline if participation is linked to a programme they depend on.

If discussion doesn't get this far it is vital to say: "What if I consented at the start, then halfway through said something I clearly regretted. What would you do with that?"

SECTION 4 — Survey design, platforms, and data storage (7 min)

Step out of character — colleague to colleague.

You mentioned sending a survey after the interview - let's discuss both how we design them and where the data goes.

Scenario prompt: Raise these as practical questions for the group to work through together.

On consent in surveys: A consent statement at the top of a survey is not enough on its own. There must be a genuine tick-box or written "I consent" before the substantive questions begin — not a statement that says "by completing this survey you are consenting to...". The survey must also tell respondents what the data will be used for, who will see it, and how long it will be kept.

On question design: Every question in a survey should earn its place. Before including anything, ask: do we actually need this? Will we use it? Could it cause harm if mishandled? Avoid collecting demographic data (age, gender, race etc) unless it is genuinely necessary for the analysis. Sensitive questions should always include an opt-out option ("prefer not to say") and should never be positioned in a way that implies they must be answered to complete the survey.

On platforms: Where does the survey data actually live? Common platforms realife may use: Google Forms, Kobo Toolbox, SurveyMonkey, Typeform - each store data on their own servers, often in the US or Europe. This has implications for cross-border transfer rules (we'll come back to this). Key questions before choosing a platform: where are the servers located? What is the platform's data retention policy? Can data be exported and deleted from the platform once collected? For projects involving particularly sensitive data or vulnerable participants, the answer to all three questions needs to be satisfactory before the survey goes out. Kobo Toolbox, for instance, offers a humanitarian server with specific data protection commitments which is worth knowing about for certain project contexts.

On moving data off the platform: Once a survey closes, export the data, store it in the agreed realife project folder, and delete it from the platform. Don't leave live data sitting indefinitely in a third-party platform you've stopped actively using.

SECTION 5 — Anonymisation and identity protection (12 min)

Back in character as the activist.

I want to be honest with you. I am scared. The work I do puts me at risk. There are people who would prefer I stopped. If I don't stop I think they might stop me. Activists are killed for so little money here. What are you going to do to make sure no one finds out what I said?

QUESTION 4: What does anonymisation actually involve — and where does it go wrong?

5–6 minutes.

Facilitator note: Anonymisation is not just removing a name. Location, specific details about someone's work, relationships, the project subject itself can all re-identify someone. The jigsaw effect: individual pieces combine to make someone identifiable even when each piece seems safe. Anonymisation doesn't end when raw data is deleted. It is a process which must be actively maintained through every subsequent piece of

writing. Stories can become non-anonymous through accumulated context. Raw data must be deleted once purposes are fulfilled. realife's default is deletion after contract completion unless otherwise specified. Physical notebooks: once contents are transferred to secure digital storage, pages should be shredded or burnt, not just binned.

If discussion stalls: "I'm the only female community leader working on water rights in a particular village. What would you need to change about how you wrote up my story?"

SECTION 6 — AI tools, storage, and security (8 min)

Still in character.

Wait. You used something called Otter AI to transcribe our call. Doesn't that mean my information belongs to some big corporation now? Are they going to use it to train their AI?

Take brief responses, then address.

Facilitator note: Otter (and Fathom's) stated policy is that data is not used to train models without user consent. However we shouldn't rely on any third-party platform's stated policies alone, as these can change and in some cases could be compromised (in some particularly sensitive situations all online data storage platforms should be assumed to be compromised by state actors and not used). The practical principle: the transcript output must be stored on realife's own systems, treated as raw personal data, and anonymised or deleted in line with our normal procedures. We can't anonymise data before it enters a live transcription tool, so the obligation falls entirely on what we do with the output afterwards.

OK. But what about until you delete my information — where is it being kept right now?

QUESTION 5: Where does raw data live, and how do you keep it secure?

3–4 minutes.

Facilitator note: Primary storage is realife's Google Drive: sensitive raw data must be in a specific project folder or in case where it should not have any administration access beyond yours then on a new shared drive with restricted access. Personal devices become data stores the moment someone writes notes on them: consider encryption, password protection, screen locks. Physical notebooks are data stores too: store securely, transfer contents, shred pages when done. Survey platform data: export, store in the project folder, and delete from the platform.

Paste into chat: https://haveibeenpwned.com/

Ask everyone to check their non-realife email addresses now - starting with the one they use the most but do all if they have multiple. Phone numbers too when they get a moment.

Facilitator note: Most people have had credentials exposed in a breach they know nothing about. Name that realife's biggest current security feature is that we're not a high-value target. However AI-enabled phishing is an increasing risk for small organisations. The most likely attack is a convincing email appearing to be from a colleague. Mention that Google passwords have never been Pwned, but many people have been hacked due to bad passwords and phishing attacks.

SECTION 7 — Photography, video, and children (10 min)

Still in character.

Actually, I want to ask you something else. You took photos at that community meeting last month. I was there. I saw them appear in an email newsletter afterwards. I didn't agree to be in a newsletter.

Step out of character.

Scenario prompt - photography and video: Ask the group — "What are your obligations when you take photographs or video in a field or workshop context?"

Key points: Images are personal data: same consent principles apply as for interviews. Group photographs make individual consent complex but the obligation still exists (but context is key - if people gather for a group photograph and you explain the purpose and use of the image so that all understand then in many cases that can be sufficient). Images shared publicly cannot be recalled, the bar for consent should be higher, not lower. If someone withdraws consent for an image after the fact, it must be removed from all uses including archived materials and past newsletters. Default: written consent for any image that may appear in communications, reports, or publications.

Brief pause, still out of character.

Scenario prompt - children and vulnerable adults: Follow on naturally: "Some of the communities realife works with include children and people in vulnerable circumstances. What changes?"

Key points: Consent for children usually requires a parent or guardian but the child's own views must be taken seriously and not overridden casually. Vulnerability doesn't remove someone's right to make decisions about their own data, it means we work harder to ensure consent is genuinely free. Revisiting consent at the end of an interaction is not optional in these contexts; it is essential.

SECTION 8 — Sharing data and partner organisations (10 min)

Still in character.

You said you're sharing what I told you with a partner organisation. I said I was ok with that — but I want to understand what that actually means. Who at that organisation? What for? Will they be looking at the recording of me?

QUESTION 6: What are your obligations when sharing personal data with a third party?

4–5 minutes.

Facilitator note: Any sharing requires knowing exactly what data is being shared, what the recipient will do with it, and ensuring they operate to the same standards as realife, agreed in advance and documented. Under POPIA, organisations including civil society partners have the same data subject protections as individuals which means information about a partner organisation itself carries data protection obligations in South Africa (when we consider the political nature of South African organisations compared to the state aligned civil society in the UK then this is a very understandable approach). Different from GDPR, where companies are generally not data subjects. Under GDPR, formal data processing agreements are required when sharing data between organisations, often not in place for smaller civil society partners, so flag this when it arises. Potential prompt: What information might be useful to protect about the organisations realife work with?

Step out of character, colleague to colleague.

Scenario prompt - cross-border transfers: "Imagine we're working on a project where interviews are conducted in Namibia, transcripts are stored on a UK-based Google Drive, and the funder is in Sweden. What do we need to think about?"

Key points: South Africa and Namibia are not currently on the UK's adequacy list, so for UK-GDPR projects, explicit safeguards are needed for data moving to Southern Africa. Under POPIA, transfers outside South Africa are restricted unless equivalent protection exists or explicit consent has been given. Know where your data is physically stored — Google Drive servers may be US or European-based. This connects to the survey platform discussion earlier. Flag any cross-border dimension to the realife data lead at project start, not retrospectively. Don't try to solve this yourself.

SECTION 9 — Secondary data (8 min)

Out of character — colleague to colleague.

Scenario prompt: "We've just received a dataset from a partner. It is survey responses they collected from community members over the past year. They've shared it because we're evaluating the same communities. What do we need to ask before we use it?"

Key points: Secondary data carries its own consent history. Key questions: what did participants consent to? Does our intended use fall within those purposes? Were they told their data might be shared with an external evaluator? If not, we either need fresh consent or we work only with anonymised aggregate data. Ask for a copy of the consent form that was used — it tells you what you can and can't do. This applies equally to monitoring databases, attendance records, beneficiary lists, and survey datasets.

SECTION 10 — Access requests and deletion (10 min)

Some time has passed. The project is ongoing. Raw data hasn't been deleted yet.

Read aloud as a message received:

"Hello, I've been thinking about our conversation. I'd like to see everything you hold about me. The recording, the transcript, any notes. Can you send it all to me?"

QUESTION 7: What are your obligations — and what do you actually do?

3–4 minutes.

Facilitator note: Under both POPIA and GDPR, individuals have the right to access their own personal data: a Subject Access Request. However we of course must check this is definitely the person! Once confirmed realife must respond within one month. The response must include all personal data held: recording, transcript, notes, survey responses, relevant emails. If this happens on a live project, contact the realife data lead immediately. Document the request and the response.

Read another message aloud:

"I need to tell you something urgent. I no longer trust the partner organisation you're working with. We've heard that someone there shared private information about another activist and that person was threatened. I want you to delete everything you have about me. Everything. And do not share anything with anyone. Please."

QUESTION 8: What do you do, and in what order?

4–5 minutes.

Facilitator note: Acknowledge receipt immediately; stop all sharing with the partner before anything else; locate all instances of their data across all storage including survey platform exports; delete all raw personal data; check whether any produced outputs contain identifiable information and redact; document what was deleted, when, and by whom; contact the realife data lead. The concern about the partner organisation is covered next.

SECTION 11 — Breach response: yours (10 min)

Out of character — colleague to colleague.

New scenario. This one is on us.

Someone on the team sends the wrong spreadsheet to a funder. It contains the names, email addresses, and approximate locations of interview participants from an active project.

QUESTION 9: What do you do — and who is it your responsibility to inform?

5–6 minutes.

Facilitator note: If sent as a Google Drive link, revoke access immediately; contact the funder, explain the error, request deletion, send the correct file, get written confirmation; if confirmation is satisfactory, document everything. This may be the end of the breach; if not, inform affected individuals using whatever channel is safest for them individually and offer practical advice. In South Africa: submit form SCN1 to the Information Regulator which is a legal requirement under POPIA. In the UK: if rights and freedoms are at risk, notify the ICO within 72 hours. Contact the realife data lead. Do not manage this quietly.

SECTION 12 — Breach response: a partner's (8 min)

Read as a message from the partner colleague.

Read aloud:

"Hi — I need to talk to you confidentially. We think we may have had a breach here. A staff member left recently and we've discovered they downloaded a lot of files before they went, including some relating to the communities we've both been working with. We're not sure what to do and we haven't told anyone yet. Can you advise?"

QUESTION 10: What is realife's responsibility here — and what do you do?

4–5 minutes.

Facilitator note: realife may have obligations to affected individuals regardless of where the breach originated, if we shared data with this partner or if the affected people are participants in a joint project. Do not investigate alone. Do not advise the partner informally on their breach response - that creates liability. Do not reassure participants that everything is fine until you know more. Contact the realife data lead immediately. The partner's breach is their legal responsibility to report, but our duty of care to our participants does not end because the breach happened elsewhere.

SECTION 13 — The contracted facilitator (10 min)

Enter character as the freelance facilitator. Signal the shift clearly.

Hi. I'm really excited about working with you on this project, delivering a Learning Landscapes session with this community group sounds like exactly the kind of work I want to be doing. I just want to check a few things before I sign so I can get stuck in.

The participant information I'll have access to: names, contact details, maybe what people have shared in previous sessions. I'll need that to plan properly. Can I keep a copy on my laptop?

Take responses.

OK, that makes sense. And during the workshop, I usually audio record sessions so I can write up my notes properly afterwards. I'd use a transcription app on my phone. Is that fine?

Take responses.

Last thing, at the end of the project I'd like to write up a case study for my portfolio. The work is interesting and I want to be able to talk about it. Can I do that?

Take responses.

Facilitator note: Risks for contracted staff include personal device storage, recording and transcription in group contexts, and post-project use of participant material. A contractor working on realife's behalf has the same data protection obligations as a realife employee. Any portfolio or case study use must be agreed with realife and the relevant partner before work begins, must not contain identifiable participant information without specific consent for that use, and should be written into the contract, not handled informally afterwards. If training associates or freelancers, spend more time here.

SECTION 14 — Outcome Harvesting and MSC (7 min or longer if relevant)

Out of character — colleague to colleague.

Scenario prompt: "We're running an Outcome Harvesting process with a partner. We've collected outcome stories from community members. These are rich, personal narratives about what has changed for them. We now need to share those stories back to the partner for verification. What do we need to check before we do that?"

Key points: OH and MSC generate some of the most sensitive data realife collects… change stories often reveal relationships, conflicts, political positioning, and vulnerabilities. Stories circulate widely: to partners for verification, to funders in reports, to sector audiences in publications. Consent given at collection may not have covered all of these uses. The verification stage is a particularly common point where this breaks down, a participant may have consented to realife using their story but not to it being read and discussed by staff at the partner organisation they named in it. Before sharing for verification: check consent scope, check re-identification risk, check the partner's data handling. Attribution in public materials is a separate consent decision from the original collection.

Additional prompt: "Imagine a story describes a community member's conflict with a specific local official. Who can currently see that story in your OH process - and does the person who shared it know that?"

SECTION 15 — Retention schedules (5 min)

Out of character — colleague to colleague.

One practical area which is vital - and varies compared to academic work in some cases: how long do we actually keep different types of data?

Walk through realife's working framework:

- Raw personal data: recordings, transcripts, original notes, identified survey responses: delete when the contract is complete and outputs signed off.
- Anonymised data and aggregated findings: can be retained for organisational learning if useful.
- Consent records: retain for the duration of the project plus two years.
- Financial records containing personal data — invoices, contracts, payroll: seven years in line with tax obligations in both SA and UK.
- Email correspondence containing personal data: review and delete after project close.
- Survey platform data: export, store in the project folder, delete from the platform — don't leave data sitting in a platform you've stopped actively using (e.g. once you have closed the survey and used any of its built-in analytical tools).
- Default: when in doubt, less time rather than more. Ask the realife data lead if uncertain.

SECTION 16 — Ethics beyond compliance (10 min)

As yourself.

Everything we've covered is about compliance, doing what the law requires, doing it carefully, not causing harm through negligence. That matters. But realife's data practice is about something more.

The way we collect, hold, and use information about people is a political act. The communities we work with have long experience of their stories being extracted, repackaged, and used for purposes that did not serve them. Evaluation and monitoring systems have historically been part of that extraction. Data has been used to justify decisions made without, or against, the people the data was about.

The activist we've been hearing from today is not a research subject. They are a knowledge holder. Their story does not become our property because they shared it with us.

Discussion question: What would it mean for realife's data practice to genuinely serve the people the data is about, not just avoid harming them?

Run for 8–10 minutes.

Threads to draw out if conversation is rich: Whose questions does the data answer? Do the people who contributed data ever see the results in a form meaningful to them? Who owns the story when it becomes a funder's case study? What does co-designing monitoring tools look like versus imposing them? What happens when funder accountability requirements and participant-centred ethics conflict? realife's Learning Landscapes frameworks name communities as primary archivists of their own knowledge, what does that mean in practice for how we handle what comes out of those processes?

If the group is quiet: "Think about the last report you contributed to. Did the people whose experiences filled it ever see it? Would they have recognised themselves in it?"

SECTION 17 — Close and next steps (5 min)

A few things to carry forward:

realife's data protection and ethical research policy. Read it. If anything in it contradicts what we've discussed today or doesn't cover your parts of work, tell me.

If you're ever unsure: a consent question, a storage question, a breach, a request from a participant - contact realife's data lead immediately. Don't resolve it alone and don't wait.

Check haveibeenpwned.com for all your email addresses and phone number if you haven't already.

Look at who has access to data you currently hold on active projects. If anyone has access who shouldn't, raise it this week.

If you're an associate or contractor: check that your data obligations in the contract are clear. If they're not, ask.

Share the recording of this session and the script document for reference.

Be ready for follow up training next year - it won't be the same as new contexts emerge for all of us. We can scenario play and check at any point too.

Further questions?

Key legal references:

POPIA / Information Regulator (SA): https://www.justice.gov.za/inforeg/

UK GDPR / ICO: https://ico.org.uk/ EU: https://gdpr.eu/