APPENDIX TO THE AI-CARES PRACTICAL GUIDE

AI Data Readiness Checklist



Are your organisation and its data ready for AI?

Tim Vanhove, Sylvie Bernaerts, Tom Seymoens,
George Caique Gouveia Barbosa, Tom Van Daele,
Jana Verplancke & Dieter De Witte

artevelde hogeschool
GHENT UNIVERSITY
THOMAS MORE
with the support of VLAIO

1

Introduction

- Why this checklist?
- Who is this checklist for?
- How to use this checklist

Why this checklist?

AI offers many opportunities for organisations in wellbeing and mental health. It can help reduce administrative workloads, streamline processes, identify patterns in data or improve the quality of support and services. But responsible AI use does not start with technology alone. It starts with data, people, agreements and responsibilities.

Before your organisation starts working with AI, you need to address some **basic questions**:

- What data do we have?
- Where is it stored?
- Is it usable and sufficiently reliable?
- Are we allowed to use it for our intended purpose?
- Who is responsible?
- Who oversees privacy and data protection?
- What agreements do we need when working with an external partner?

These questions are especially important when you work with **personal data**. In wellbeing and mental health, this often involves information about people in vulnerable situations. It may also involve special categories of personal data, such as health data or information about mental wellbeing. Careless use of this data can affect people's privacy, trust, rights and safety.



This checklist helps your organisation assess, step by step, whether the basic conditions are in place to work responsibly with data and AI. The focus is not on the AI technology itself, but on what you need before starting an AI project:

1. Clear roles and responsibilities
2. An overview of what data is available, where it is stored and in what form
3. Clarity about what is legally permitted and under which conditions
4. Attention to anonymisation and pseudonymisation for the protection of the individuals concerned
5. Agreements on sharing data with external partners

The aim is not to answer every question perfectly straight away. Above all, this checklist helps you understand where your organisation currently stands, which gaps remain and what steps to take next. Use it as a practical guide and a starting point for discussion within your organisation.

Disclaimer

This checklist has been developed as an informative and practical resource, based on the information and insights available at the time of writing. Although the content has been compiled with care, the checklist may not be exhaustive or applicable to every situation. It does not replace legal advice or an assessment by your DPO, legal adviser or person responsible for privacy. The authors cannot be held liable for the use of this checklist or for decisions made on the basis of this information.

Your organisation remains responsible for assessing whether a proposed AI application is legally, ethically, technically and organisationally appropriate, and for consulting all relevant internal or external experts at an early stage.

Who is this checklist for?

This checklist is intended for organisations in wellbeing and mental health that work with personal data. This often includes sensitive data, such as information about health, mental wellbeing, support needs, family circumstances or other personal circumstances of clients, users, patients or members of the public.

The checklist is designed for organisations that want to explore, prepare for or introduce AI and data-driven applications responsibly. It helps you gain a clearer understanding of the data, roles, agreements and conditions needed before you begin. It is intended for anyone involved in AI-driven innovation, including:

- Senior managers and policy staff
- Project leads
- Data stewards or staff responsible for data
- IT staff
- Quality assurance staff
- Staff responsible for privacy
- Innovation staff

You do not need to be a legal, technical or AI expert to use this checklist. It is intended as an accessible starting point for discussion within your organisation. It helps bring together perspectives from practice, policy, IT, data management, privacy and innovation.

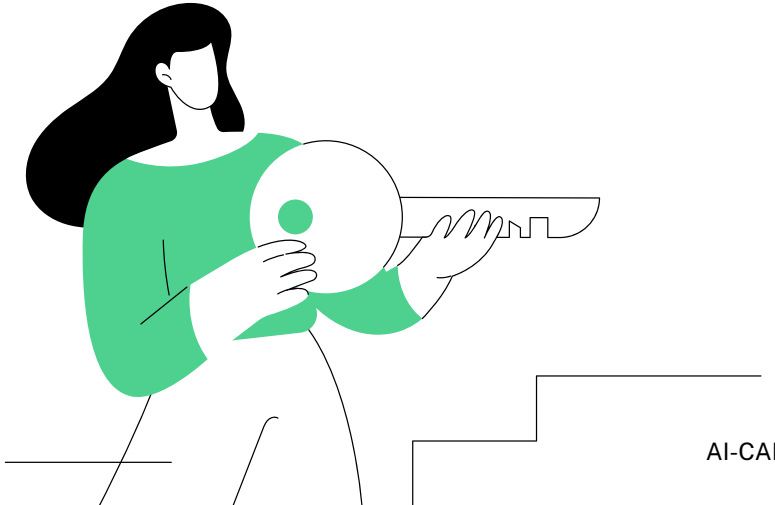
The checklist does not provide a definitive legal assessment. It does help you prepare for discussions with your DPO, legal adviser or person responsible for privacy.

How to use this checklist

This checklist helps your organisation assess whether the basic conditions are in place to work responsibly with data and AI. Start with a specific need, question or opportunity for improvement within your organisation. Which process is not working well? Which task takes a lot of time? What information is missing? Where do staff, clients, patients, members of the public or users encounter recurring problems?

The checklist helps you assess whether your organisation is ready to explore implementing an AI application responsibly. It covers five themes that together provide a sound basis for responsible data use and AI applications:

1. **Roles:** Who needs to be involved, and who takes on which responsibilities?
2. **Data:** What data is available, where is it stored, in what form does it exist, is it usable?
3. **Legal requirements:** May we use this data for our intended purpose, and under which conditions?
4. **Anonymisation and pseudonymisation:** How do we protect the people behind the data and reduce the risk of identification?
5. **Data sharing:** What agreements are needed when sharing data with external partners, such as researchers, developers or technology partners?



Describe the AI application you want to explore: an example

Before completing the checklist, briefly describe the AI application you want to explore. For example: analysing chat conversations to better understand recurring support needs.

What do we want to do with AI?

We want to investigate whether AI can help identify patterns in chat conversations with clients. Which topics come up frequently, which questions are often asked, when do clients seek support, and which needs may not yet be adequately addressed?

Who is the application intended for?

The application is primarily intended for the organisation itself: policy staff, coordinators, quality assurance staff and practitioners who want to improve services. It is not intended to assess individual clients or make automated decisions about them.

What added value do we expect?

We expect to gain a clearer picture of recurring support needs and possible gaps in the services offered.

Bring together colleagues who can each consider the questions in this checklist from their own area of expertise: practice, policy, IT, data, privacy, quality and innovation. The value lies not only in completing the questions, but above all in the discussion they generate.

Starting from your proposed AI application, work through what data is needed, who should be involved, what needs legal review and which agreements are required. This will clarify where you currently stand, which questions have already been answered, where gaps remain and what action is needed before you move forward.



2

Checklist

- Question 1: Who should you contact?
- Question 2: What data do we have, where is it stored and in what form?
- Question 3: What is permitted, and under what conditions?
- Question 4: How do we protect the people behind the data?
- Question 5: Can we share our data?

QUESTION 1

Who should you contact?

THE ROLES

AI projects that use data require more than good technology. You also need to know who should be involved and who is responsible for what. Who knows the data? Who understands the practice from which it originates? Who oversees privacy and data protection? Who knows the technical systems? Who knows the agreements with suppliers, partners or platforms? And who has the authority to make decisions about data use, collaboration or risks?

DPO, legal adviser or another authorised person

First, check whether your organisation has a DPO. A Data Protection Officer helps oversee data protection and advises on privacy, the European GDPR rules on privacy, lawful bases, data sharing and risks to the individuals concerned. The DPO has an independent advisory and monitoring role. They provide advice and oversight but are not responsible for making operational decisions about an AI project. Not every organisation is required to appoint a DPO. Even if your organisation does not have a formally appointed DPO, it is important to know who you can contact internally or externally about privacy and data protection. This could be a legal adviser, a person responsible for privacy or an external adviser.

Please note: not every legal question is automatically a question for the DPO. For matters concerning usage rights, licences, supplier contracts or collaboration agreements, you also need to know who can help review them. This may be a legal adviser, but it could also be someone working in procurement, contract management, policy or project coordination.

Data steward

It is also useful to appoint a data steward or someone who can connect different teams and areas of expertise in your organisation. This person helps maintain an overview: they understand the needs of practitioners and can also engage with IT, policy staff, legal advisers and external partners. This role can make a significant difference to the success of data-driven projects.

This person does not have to be a data specialist but needs a sufficient understanding of how the organisation works, where data is generated, who uses it and which questions arise in practice. This data steward helps bring the right people together and prevents data and AI questions from being left solely to IT or policy staff. Even if you have a DPO, a data steward remains valuable because of their accessibility and practical focus.

Data administrator

You also need someone who understands the technical side, usually a person with IT skills: a data administrator. This person knows, for example:

- Which systems store the data
- Who has access
- Whether the data can be exported securely
- What technical limitations apply
- What needs to happen if there is a technical problem or security incident

Decision maker with the necessary authority

Finally, it must be clear who is authorised to make decisions. AI projects involve choices about priorities, resources, collaboration, risks and responsibilities. Make sure it is clear who has the authority to start, modify or stop an AI project, and who can decide when to involve internal or external experts.

CHECKLIST

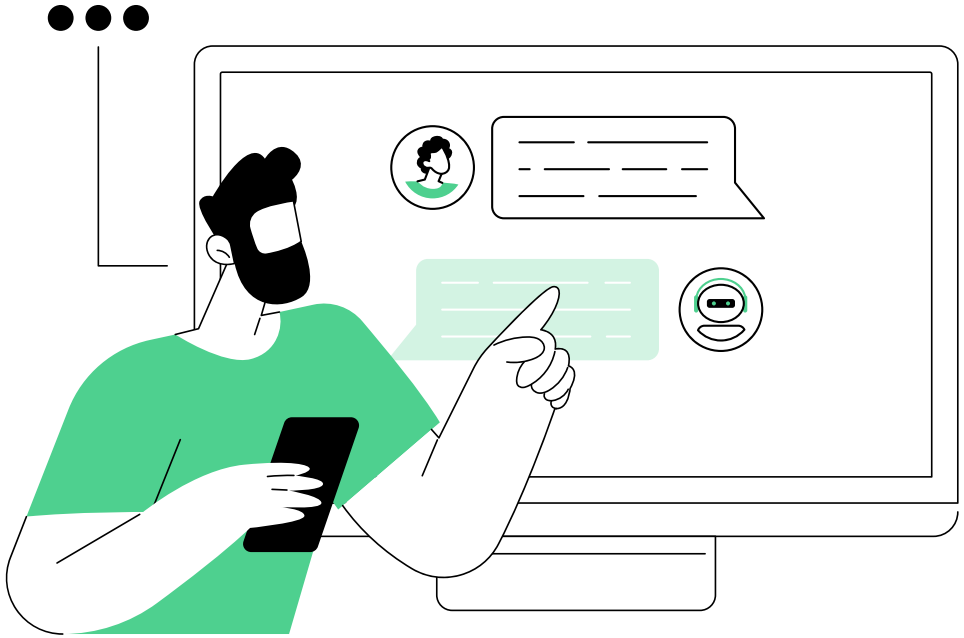
- ☑ We know who we can contact internally or externally with questions about privacy and data protection. We know whether our organisation has a DPO and how to contact that person.
- ☑ We know who can help review contracts, licences, terms of use or agreements with suppliers and partners.
- ☑ We know who can connect the needs of practitioners with IT, policy and privacy considerations (data steward).
- ☑ We know who has a technical overview of our systems, databases, platforms, access arrangements and exports. We know who to contact if something goes wrong with data, access, security or data sharing (data administrator).
- ☑ We know who has the authority to make decisions about data use, AI applications or collaboration with external partners (decision maker).
- ☑ We have collected these people's names, roles and contact details in one place.

First step

Are there still items you cannot tick off? This gives you a starting point: either nobody has yet been assigned to a particular role, or it is not clear to everyone who performs it.

Create a simple overview of roles. Check at least:

1. Who helps review privacy and data protection matters?
2. Who knows the contracts, licences or agreements with suppliers, partners or data providers best?
3. Who has the best technical knowledge of our systems and data?
4. Who understands what the data means in practice?
5. Who maintains the overview and brings the right people together?
6. Who can decide whether we proceed with an AI project, data exchange or an external partner?



QUESTION 2

What data do we have, where is it stored and in what form?

THE DATA

Before you can start working with AI, you need to know what data your organisation has. Data comes in many forms: chat conversations, client files, records, manuals, internal documents, reports and more. An overview is therefore essential: where is the data? In which system or platform is it stored? Who has access? Can you export it? And in what form will it be exported?

Not all data is immediately suitable for AI. Sometimes you can only download it as a PDF, even though you need the data in a different format, such as structured text or a spreadsheet. Sometimes the data is incomplete, recorded inconsistently or difficult to interpret without knowledge of the practice.

Data quality also matters. A common saying in the data field is “garbage in, garbage out”. If the data is incomplete, poorly organised or unclear, the output of an AI application will also be less reliable.So don’t just check whether the data exists. Check whether it is sufficiently complete, consistent and understandable for your intended purpose.

At this stage, your main task is to identify what data exists and whether it might be usable. This does not mean you are already permitted to copy, export, analyse or share it. You will explore whether this is legally permitted later in the checklist, together with your DPO or legal adviser.

CHECKLIST

- ☑ We know what data may be relevant to our proposed AI application.
- ☑ We know in which systems, platforms or files this data is stored.
- ☑ We know who has access to this data.
- ☑ We know who understands what this data means in practice.
- ☑ We know the form in which the data is available, for example text, tables, PDFs, export files, free text or fixed fields.
- ☑ We know whether the data can be exported.
- ☑ We know whether the data is structured, for example in tables or fixed fields, or consists of free text, such as emails, reports, case files or chat conversations.
- ☑ We know whether the data is sufficiently complete for our intended purpose.
- ☑ We know whether the same information is recorded consistently.
- ☑ We know who can help if data is incomplete, unclear or difficult to export.

First step

Create a simple data inventory for your proposed AI application.
Check at least:

1. What information do we actually need for this application?
2. Where is that information stored?
3. Who has access?
4. In what form does the data exist?
5. Can the data be exported?
6. Who understands what the data means in practice?
7. What limitations or quality issues can we identify?

QUESTION 3

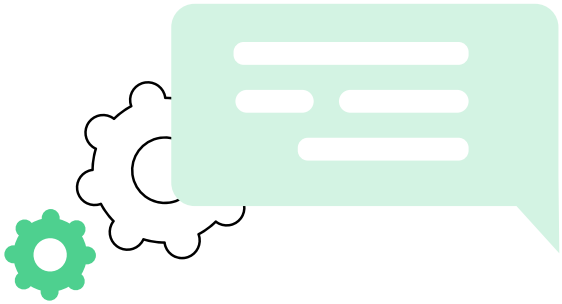
What is permitted, and under what conditions?

LAWFUL BASIS

If you want to use data for AI tools, research, quality improvement or collaboration with an external partner, you need to establish whether this is legally permitted. Good intentions are not enough: you must be able to explain what you want to use the data for, why this is necessary and under which conditions it can be done.

You need to consider at least two questions. First: may you process personal data under data protection rules? Second: may you also use the data, database or content under the applicable usage rights, contracts and licences?

You do not have to make this legal assessment alone. Involve your DPO, legal adviser or person responsible for privacy. What you can do is prepare the right questions.



Data protection

An important first question is: what did we originally collect this data for, and do we now want to use it for the same purpose or for something new?

Information collected during a conversation with a client, user, patient or member of the public cannot automatically be reused for AI development or other purposes. Particular care is needed with client information, requests for help and health data.

Every step of processing personal data requires a valid lawful basis. Organisations sometimes think: “We will ask users for consent.” That is possible, but consent is only one potential lawful basis. The appropriate basis depends on the purpose, context, type of data, relationship with the individual concerned and your organisation’s statutory responsibilities.

If you rely on **consent**, it must be freely given, specific, informed and unambiguous (“informed consent”). The individuals concerned must understand what their data will be used for and have a genuine choice. Consent to receive support or help is not automatically consent to reuse that data in an AI project. When processing special categories of personal health, additional legal conditions apply. Consult your DPO or legal adviser to determine which conditions must be met.

Check what clients, patients, users or members of the public have already been told about the use of their data. Does the **privacy notice** explain why data is collected and used? Does it mention use or reuse for research, quality improvement or development? Is it clear whether data may be shared with external partners? Are the rights of the individuals concerned explained?

If this is unclear, do not simply proceed. First gather the necessary information and raise the question with your DPO, legal adviser or person responsible for privacy. You may need to change your organisation’s privacy notice. You may then only use data collected after the new privacy notice came into effect. Updating your privacy notice does not automatically make the intended data use lawful. Consult your DPO or legal adviser to determine whether previously collected data can be reused and under what conditions.

Usage rights and licences

In addition to data protection, you also need to check whether the applicable usage rights, contracts and licences allow you to use the data or content. Not everything that is technically available may simply be copied, exported, shared, enriched or used for AI. This is relevant, for example, when data comes from an external platform, a commercial tool or material supplied by an external organisation. You therefore need to check whether copyright, licensing terms or contractual agreements apply: who holds the rights to the content, what does the supplier contract say, and is export for use with an external partner permitted?

Usage rights and licences address different questions. For data protection, you ask: may we process personal data for this purpose? For usage rights and licences, you ask: do we have the right to use this data, database or content in this way?

Please note: this checklist helps you ask the right questions, but it does not replace your organisation's responsibility to ensure compliance. Your organisation remains responsible for using personal data, sensitive data and AI applications in a legally GDPR-compliant and ethically responsible way. Involve your DPO, legal adviser and other authorised staff well in advance, particularly when the proposed AI application could affect clients, patients or users.

CHECKLIST

Original use

- ☑ We know why the data was originally collected.
- ☑ We know the lawful basis on which the data is processed.
- ☑ We know what clients, patients, users or members of the public were told about this in our privacy notice.

New use

- ☑ We know what we now want to use the data for.
- ☑ We have checked whether this new use is compatible with the original purpose.
- ☑ We have checked whether this proposed AI application requires a new or additional legal assessment.

Type of data

- ☑ We know whether the data includes personal or sensitive data, such as health data or information about mental wellbeing.
- ☑ We know whether the data or content comes from an external platform, database, tool, questionnaire, methodology or material supplied by an external organisation.

Information provided to the individuals concerned

- ☑ We have checked whether our privacy notice describes this use clearly enough.
- ☑ We have checked whether existing consent wording or information sheets adequately cover this use.

External use or sharing

- ☑ We know whether the data will remain within the organisation or be shared with an external partner.
- ☑ We know whether an external partner processes the data only on our behalf or also has a say in deciding what happens to it.

Usage rights and licences

- ☑ We have checked whether our contracts allow us to use the data for this new purpose.
- ☑ We have reviewed the relevant agreements, licences or terms of use with partners, suppliers or data providers.
- ☑ We have checked whether reuse for AI, research or quality improvement is permitted.
- ☑ We have checked whether contractual restrictions apply to copying or exporting data, sharing data, combining or enriching data, training or testing AI models, publication, commercial use or other activities.
- ☑ Where necessary, we have amended or extended contractual arrangements before using the data.

DPO check

- ☑ We know which questions we need to put to our DPO, legal adviser or person responsible for privacy.
- ☑ We do not proceed with using, exporting, analysing or sharing personal data until it is clear whether this is legally permitted.
- ☑ We do not proceed with using, exporting, analysing or sharing data until it is clear whether usage rights, licences or contractual agreements allow this.
- ☑ We have discussed with our DPO, legal adviser or person responsible for privacy which obligations under the EU AI Act may be relevant to this proposed AI application.

First step

Review your proposed AI application alongside the following documents or information sources:

1. The privacy notice
2. Any informed consent wording or information sheets
3. The data processing register or Record of Processing Activities (RoPA)
4. Relevant contracts with suppliers, partners or data providers

Then answer these questions together with your DPO, legal adviser, person responsible for privacy or another authorised person:

- ☑ Why was the data originally collected?
- ☑ What do we want to use the data for now?
- ☑ Do the individuals concerned know that their data may be used for this purpose?
- ☑ Does it involve personal or sensitive data?
- ☑ Do the contracts, licences or terms of use allow us to use the data for this new purpose?
- ☑ May the data be shared with an external partner?
- ☑ May the data be used for AI, research, development or quality improvement?
- ☑ Does our DPO, legal adviser, person responsible for privacy or contract manager need to assess this before we proceed?

If the answer to any of these questions is unclear, do not yet proceed with using, exporting or sharing the data. First identify what needs to be changed or legally reviewed.

QUESTION 4

How do we protect the people behind the data?

ANONYMISATION AND PSEUDONYMISATION

Organisations in wellbeing and mental health often work with data about people in vulnerable situations. This includes clients, patients, users or members of the public who seek help, share personal information or receive support. This is not just data. It is information about real people. Careless use can affect their privacy, trust, rights and safety.

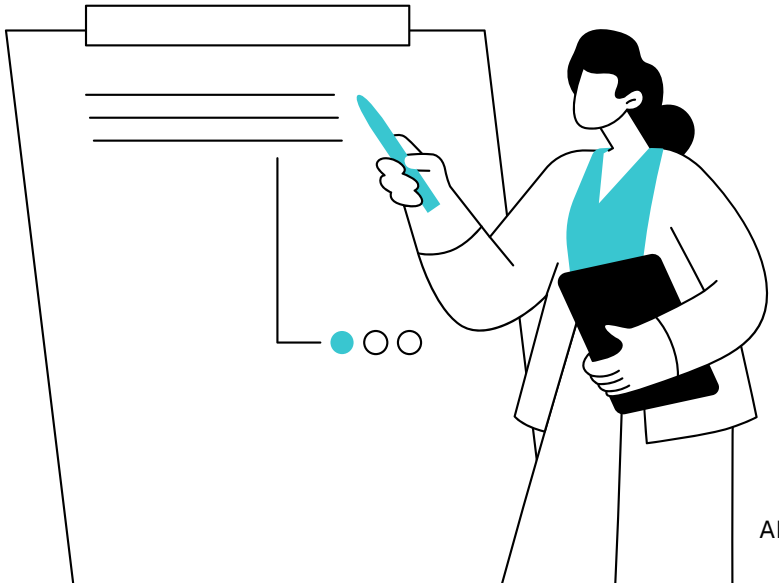
You therefore need to assess whether people can still be identified in the data you want to use. This is not always straightforward. Even if you remove names, email addresses or phone numbers, people may still be identifiable through details in their personal circumstances. Examples include a place of residence, school, age, family circumstances, a rare event, a role or a combination of these characteristics. If someone could reasonably be identified by putting a few 'pieces of the puzzle' together, the data cannot be considered fully anonymous.

Free text often contains more identifying information than you might initially notice. A client may not mention a name but may refer to a small town, a specific school, particular family circumstances or a recognisable event. Removing names alone is therefore usually not enough. You also need to consider indirectly identifying details and combinations of data.

Removing names is not the same as anonymisation

Data may appear anonymous because direct identifiers, such as names or contact details, have been removed. However, someone may still be identifiable through other information in the text or combinations of data. It is therefore important to understand the difference between personal data, pseudonymised data and anonymous data.

- **Personal data** is data that allows someone to be identified directly or indirectly. This may be a name or email address, but it may also be chat conversations containing personal details.
- **Pseudonymised data** is data in which identifying information has been removed, replaced or protected, for example by a code, but which can still be linked back to a person using a key file or by combining it with other information. Pseudonymised data therefore remains within the legal category of personal data.
- **Anonymous data** is data from which it is no longer reasonably possible to identify the person concerned. This is a high threshold. Full anonymisation is often difficult, particularly for free text such as chat conversations, client files, reports or requests for help.



Type of data	Meaning	Example	May the data be shared?
Personal data	Data that allows someone to be identified directly or indirectly.	A chat conversation containing a name, email address, IP address or identifiable personal details.	No.
Pseudonymised data	Identifying data has been replaced or removed, but the original personal data can (theoretically) be reconstructed using additional information, keys or context.	A chat conversation without personal names, but including age, place of residence, school and specific circumstances. Someone could identify the person by putting these pieces together.	Only with the appropriate agreements and measures in place. These arrangements are set out in a legal agreement (see below).
Anonymous data	It is no longer reasonably possible to identify the person concerned.	Aggregate figures only, such as the number of conversations per month for each topic.	Yes. Anonymous data does not fall under the European GDPR rules on privacy.

Protect the key as well

Pseudonymisation sometimes involves a key file. This is a separate file that allows a code to be linked back to a person. For example, “User 123” is linked in a separate file to a name, case file number or other identifying information. Such a key file must be kept strictly separate, stored securely and accessible only to a limited group. Only people with a clear reason and the necessary authorisation may access it.

Responsibility lies with the organisation

The responsibility for protecting data rests with the organisation and its partners, not with the client, patient, user or member of the public. You cannot expect people to avoid sharing personal information when seeking help or support.

Do not decide on your own whether data is sufficiently anonymous. Involve your DPO, legal adviser, person responsible for privacy or a data protection expert, particularly when working with chat conversations, client information, health data or other sensitive data.

CHECKLIST

Identifiability

- ☑ We know whether the data contains personal or sensitive data. We have checked whether people can be identified directly, for example through a name, email address, phone number, case file number or IP address.
- ☑ We have checked whether people could be identified indirectly through details in the text, the context or combinations of data.

Anonymisation or pseudonymisation

- ☑ We know which data is unnecessary and should therefore be removed or protected.
- ☑ We know whether the data can be made fully anonymous or can only be pseudonymised.
- ☑ We know which personal data needs to be removed, replaced or protected before the data is used or shared. We know that removing names does not automatically make data anonymous.
- ☑ We know whether free text - such as chat conversations, case files, reports or requests for help - needs additional checks for identifying details.

Access and security

- ☑ We know who has access to the original data.
- ☑ We know who has access to the pseudonymised or anonymised data.
- ☑ We know whether a key file exists that allows data to be linked back to individuals.
- ☑ We have agreements about who can access that key file and how it is secured.

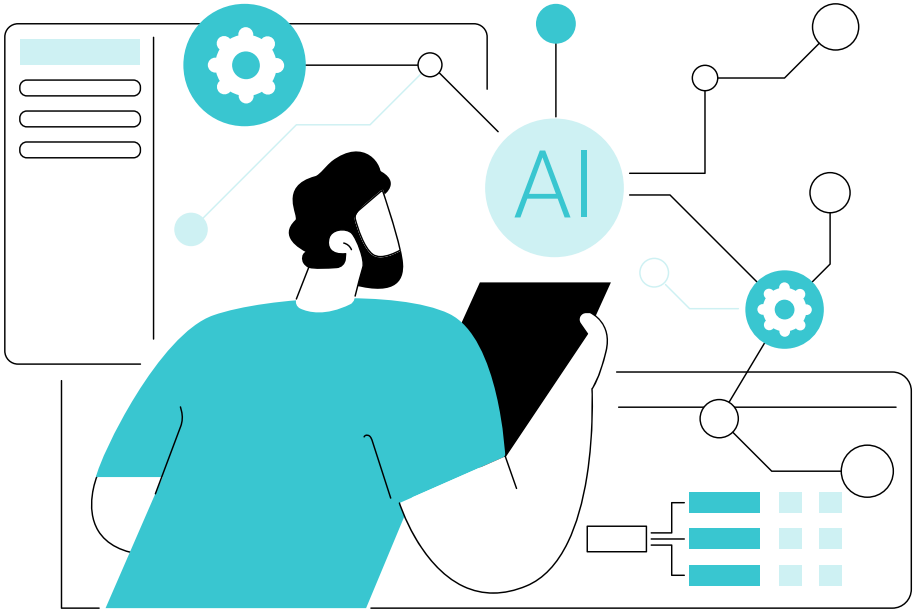
DPO check

- ☑ We have discussed with our DPO or legal adviser whether the data is sufficiently protected for its intended use.
- ☑ We do not proceed with using, analysing or sharing sensitive data until it is clear whether the protection is adequate.

First step

Take a few examples of the data you may want to use, such as a chat counselling transcript, case report, record or export file. Review the following questions together with colleagues from practice, ITn data and privacy:

- ☑ What direct identifiers does the data contain?
- ☑ What indirectly identifying details does it contain?
- ☑ Which combinations of data could identify someone?
- ☑ Which data do we actually need for our proposed AI application?
- ☑ Which data can we remove, replace or protect?
- ☑ Is anonymisation realistic, or is pseudonymisation more likely?
- ☑ Who needs to assess this before we proceed?



QUESTION 5

Can we share our data?

DATA SHARING

AI projects often involve collaboration. You may be working with a research partner, technology partner, software developer, university of applied sciences, university or external supplier. Whenever an external party gains access to data, you need to understand how that data will be used. Data sharing does not only mean sending a file. Providing access to a platform, working in a shared cloud environment, having data analysed by an external partner or running a tool on your data can also mean that personal data is being processed externally.

You need clear agreements in advance, particularly for personal data, chat counselling conversations or other sensitive data. You need to know what data will be shared, with whom, for what purpose, on what lawful basis and through which channel. You also need to know who will have access and what will happen to the data afterwards.

Start by clarifying roles

Not every external partner has the same role. Sometimes an external party processes data only on your organisation's behalf. Examples include a supplier that manages a tool or a developer building an application for you. In that case, a **data processing agreement** is required.

In other cases, the external partner also helps decide what happens to the data, for example in certain forms of research or joint development. A different agreement may then be needed, such as a **collaboration agreement, data sharing agreement or data transfer agreement**. Do not determine this on your own. Ask your DPO or legal adviser to assess each party's role and which agreement is required.

Check the data processing register

Also check whether the data sharing is included in the **data processing register** or the European Record of Processing Activities (RoPA). This documents which personal data your organisation processes, for what purpose, on which lawful basis, who has access, with whom the data is shared and how long it is retained. If you use data in a new way, share it with an external partner or have it processed by an AI tool, you need to check whether the data processing register should be updated before you start.

Share only what is needed

Do not share more data than is needed for the proposed AI application. The less sensitive or identifiable data you share, the lower the risk. Always ask:

- What data does the external partner actually need?
- Could less data be sufficient?
- Could anonymised or pseudonymised data be used?
- Do certain fields, texts or details need to be removed?
- Does the partner need access to the data, or would a limited export be sufficient?

Use a secure channel

Do not simply share personal data through ordinary email, shared folders or informal transfer services. Use only channels and environments that your organisation has approved and that are sufficiently secure. Also agree on access arrangements. Who may see the data? For how long? May the data be downloaded? Is access logged? And who revokes access when the collaboration ends?

Plan for the end of the collaboration

Agree in advance on what happens afterwards. Will the data be deleted, returned or retained? Who confirms that the data has been deleted? How long may results or derived files be retained? And what happens if something goes wrong, such as a data breach or misuse?

Checklist

Purpose and data

- ☑ We know why the data would be shared or processed externally.
- ☑ We know what data is actually needed for this purpose.
- ☑ We have checked whether less data would be sufficient.
- ☑ We have checked whether the data can first be anonymised or pseudonymised.

Parties and roles

- ☑ We know which external partner or partners we want to work with.
- ☑ We know the role of each partner: data processor, data controller, joint controller or research partner.
- ☑ We had the allocation of roles reviewed by our DPO, legal adviser or person responsible for privacy.

Legal agreements

- ☑ We know whether the data processing is included in the data processing register (European Record of Processing Activities) or needs to be added.
- ☑ We know which agreement is needed, such as a data processing agreement (DPA), collaboration agreement or data transfer agreement (DTA).
- ☑ We have agreements on the purpose of processing, permitted use, access, security, retention period and deletion.
- ☑ We know whether the external partner may engage sub-processors or other third parties.

Secure transfer and access

- ☑ We know which secure channel or platform may be used to share the data.
- ☑ We do not share sensitive or personal data through email, shared folders or transfer services without appropriate security.
- ☑ We know who will have access to the data.
- ☑ We have agreements on logging, download permissions and revoking access.

After the collaboration and in the event of incidents

- ☑ We have agreements about what happens to the data afterwards.
- ☑ We know who confirms that data has been deleted, returned or securely retained.
- ☑ We know what needs to happen if something goes wrong, such as a data breach, inappropriate access or misuse.

DPO check

- ☑ We involve our DPO, legal adviser or person responsible for privacy before data is shared or an external partner is given access.
- ☑ We do not proceed with sharing, exporting or having personal data processed externally until it is clear which agreements and security measures are needed.

First step

Before sharing data, prepare a brief data-sharing plan. Check at least:

1. What data do we want to share or have processed externally?
2. Why is this necessary?
3. Which partner do we want to work with?
4. What role does that partner have?
5. Which agreements are required?
6. Through which channel or platform will the data be shared?
7. Who will have access?
8. What will happen to the data afterwards?
9. Who needs to approve this before we start?

Submit this plan to your DPO, legal adviser or person responsible for privacy before you export data, share it or grant access.



3

Glossary

Glossary

- **Personal data:** Any information that can identify a specific person. This includes not only a name and address, but also a nickname combined with an age and a city, an IP address or a story containing enough specific details, including a case file or counselling conversation.
- **Special categories of personal data:** A specific group of sensitive data to which the European GDPR applies particularly strict rules. Examples include data about health, mental wellbeing, sexual orientation or ethnic origin.
- **Data controller:** The organisation that decides why and how personal data is collected and used
- **Data processor:** An external party that processes personal data on your organisation's behalf but does not itself decide what happens to it.
- **DPO:** The Data Protection Officer or person responsible for protecting privacy. An internal or external person who oversees your organisation's compliance with the GDPR.
- **Data steward:** The data steward maintains the day-to-day overview of data within the organisation: what is stored where, who has access and how it is used.
- **Record of Processing Activities:** An internal and mandatory data processing register, that includes what personal data is processed, why, for how long and who has access to it..
- **Lawful basis:** The legal basis that permits you to process personal data. Without a lawful basis, you may not do anything with personal data. For organisations in wellbeing and mental health, the most relevant bases are consent, public interest and scientific research.
- **Consent:** A person's explicit, freely given and informed permission to use their data. Consent to a conversation is not automatically consent to use that conversation in a research project.
- **Consent form:** The document through which a user consents to the use of their data. If you want to use their data for research or share it with an external partner, this must be explicitly stated in the consent form.
- **Anonymisation:** The process of modifying personal data so that it becomes impossible to identify the person concerned, even with additional information.
- **Pseudonymisation:** The process of modifying personal data so that as many identifying elements as possible are replaced or removed. However, the data can, in theory, still be traced back or reconstructed if enough context is available. Pseudonymised data remains subject to the European GDPR privacy regulations.
- **Data processing agreement (DPA):** A contract between your organisation and an external party that processes data on your behalf, such as the company that manages a chat or email platform or develops an AI tool.
- **Data Transfer Agreement (DTA):** A contract specifically covering the transfer of data from one organisation to another, for example to a research institution. It may also form part of a broader collaboration agreement. It sets out who does what, for which purpose and under which conditions.

www.arteveldehogeschool.be/ai-cares