DIGITAL AND
POPULATION DATA
SERVICES AGENCY

Utilisation of AI - Guidelines and Checklists

VAHTI Best Practices Support Material

13 June 2024 version 2.5

Table of Contents

Utilisation of AI - Guidelines and checklists

1. Introduction

This support material has been prepared for public administration organisations to promote secure work and activities. The VAHTI Good Practices support materials are based on recommendations and good practices compiled by the expert groups of the Finnish Public Sector Digital Security Management Board (VAHTI, https://dvv.fi/vahti) in the areas of risk management, continuity and preparedness, competence development, ICT services, information security and data protection. By complying with these, we also promote the implementation of cyber security.

The VAHTI Good Practices support materials are primarily intended for public administration organisations, but they are freely available to any organisation. We hope that if you develop or improve these materials, you will also give feedback to help us further develop the content. We welcome suggestions for improvements and corrections, and we will release an updated version once we have received a sufficient amount. You can send feedback: digiturva@dvv.fi - write "AI Best practices" in the heading.

The first version of this document was formed by using e.g. artificial intelligence, and it was published on 15 June 2023. The first version developed further by experts (1.0) was published on 12 September 2023. On 17 November 2023, 100 experts from VAHTI working groups and the Digital and Population Data Services Agency participated in the development of version 2.0, and it was published on 12 December 2023. Updates have been made to the structure of the lists in version 2.0, and the listed items are numbered to facilitate references (the numbers do not denote priority or similar). A summarised set of slides has been produced of the guideline as was requested during the workshop.

Version 2.5, published on 13 June 2024, is based on the updated version on the basis of the version prepared by the preparatory working group on the basis of the preliminary survey open to all.

We utilise artificial intelligence tools in the production of the VAHTI good practices support materials as we have with previous versions. All content goes through a review and comment process described in this document.

Dissemination of publication: Digital Security Publications | Digital and population data services agency (dvv.fi)

2. Guidelines and checklists

Organisations are free to utilise, adapt and modify the guidelines in this material intended for guidance, communication, and training of different groups of actors. The guidelines serve as checklists on issues identified as being priorities, but do not necessarily cover all the perspectives that different organisations may encounter.

Organisations must provide more detailed instructions on AI services approved for use and on their safe use. Each organisation and expert is responsible for ensuring that the contents of this support material are applied in a manner that aligns with the organisation's own industry and relevant legislation. Materials may not be used as such without a review, editing for the organisation's own specific purposes and its related appropriate communication in the organisation and, if necessary, to its stakeholders.

There is no one clear definition for artificial intelligence. Below is a list of four key observations related to its activities:

- Artificial intelligence is a **computer program** designed for a specific use.
- In order to **function, it requires a computer**, that is, a processor or a huge number of processors or other GPUs, ram and auxiliary memories (disk system) to process and store data, high-performance data connections and other technologies. Meaning bits, "iron" and electricity.
- **Artificial intelligence has no emotions, awareness, and self-awareness**, but it can act all of these on request and can, in other respects, try to act in the same manner as people, even incorrectly, on request. Artificial intelligence is a kind of actor when necessary.
- All the information it produces - images - music - videos - speech is based on **teaching data** produced by us people - from which it creates answers based on **mathematical models, probabilities**, - somewhat like predictive text input on smart devices.

In this material, artificial intelligence refers broadly to systems, processes and services that make use of AI and, in some cases, to highly developed systems in which algorithms or design are complex enough to be comparable to AI or may appear to be comparable.

This broader definition aims to include different definitions in a comprehensive manner and to draw attention to how rapidly AI-related technologies are evolving and how their effects extend for a long time and to different levels. Thus, there is no single "average" artificial intelligence.

Different use cases can be seen to involve different functionalities, threats, administrative structures, regulation, and expectations, etc. These various perspectives create different ways of classifying artificial intelligence, which are ways of communicating about related matters. Each organisation decides independently which of these are selected for use and the instructions that are provided on their use.

The organisation's use of artificial intelligence should be systematic, guided, and consistent. Artificial intelligence is already seen as such significant ICT technology that it will affect organisation-level objectives and functional capacity. Thus, organisations should have a plan for AI as a guiding practice, regardless of whether the organisation is at the forefront of its deployment or only among the last to utilise it. Artificial intelligence will be used around this plan, existing tools and systems will be saturated with it, and artificial intelligence will be used against it. Artificial intelligence will at some point in time become part of the normal operations of all organisations, which will require changes and the management of its implementation. This can be compared in part to the evolution of services used via the internet and the services produced using various smart devices, especially in the early 2000s.

Thus, in order to support the organisation's guidance, it is recommended that a plan is established for AI. It is recommended but at the organisation's discretion, whether to do this at the strategic and policy level, so that these are also developed separately before they are added to the organisation's normal overall strategy and policy. In other words, the AI strategy and policy should be formulated with the aim that they can be incorporated into normal management and activities (after the maturity of policies, technology and expertise has developed).

As the basis for AI development, the organisation should jointly, under the guidance of management, identify the potential impacts of AI on internal and external activities and the operating environment so that these can be anticipated. The strategy should tell the organisation such things as what AI is for the organisation, what the organisation is aiming for by using AI, how AI will help in achieving the organisation's goals and how to proceed from separate AI guidance to internalised normal activities. The organisation's AI policy should describe how the strategy's goals can be achieved, what AI can be used for and what it cannot, how AI activities are managed, how AI is used in the organisation, how the impacts of AI are handled and what preparations will be made for operating without AI.

The lists presented in this document need these guidelines to be established. An organisation's strategy and policy on AI activities must be maintained and updated as the capabilities of technologies and systems change, as legislation and other regulation develops, and on the basis on the benefits and disadvantages identified in the use of AI. The distinction between strategy and policy is not always clear and organisations can have different administrative cultures in place for defining these contents, which is why the division given in the guidelines can only be viewed as indicative.

2.1 Guidelines for an organisation's management

1 **Get training and familiarise yourself** with the basics of artificial intelligence from different perspectives, take it to the management's agenda and keep it there in the future. Maintain your competence.

- Prepare a vision, plan, roadmap, strategy and/or policy to support your organisation's activities, involving as many different parties as possible.

2 **Define** the roles, responsibilities and resources related to artificial intelligence and its **budgeting**.

- **Appoint** a management representative and expert(s) who will be responsible for AI management and ensure that those responsible for the acquisition, development, risk management, business continuity, information security and data protection of the organisation's applications are familiar with the policies and development projects related to the AI services developed or utilised by the organisation.
- **Ensure** that the organisation has its own or separately acquired **special expertise** in legislative changes and other new situations and phenomena occurring around AI. **Assign** sufficient reservations to experts and users responsible for AI training.

3 **Ensure** that the **risk management model** used by the organisation is applied in the utilisation of AI and the development of services, and that the identified risks are processed and managed.

- **Stay aware** of the development of risks in a rapidly evolving field and examine them extensively, in the entire service or process chain, including the subcontracting and supply chain networks related to the entity in which AI is included.
- Ensure **cooperation** with stakeholders and strive for common policies.
- Assign **responsibility** for the management of accountability for the sections of agreements that concern AI.
- **Ensure** that the organisation has the opportunity to explore and test AI in its various forms safely to identify its potential. Also prepare for the management of any realised risks.

4 **Plan and implement change management and communication** when entities related to or including AI are implemented (e.g. impacts on work, client services, stakeholders).

- **Ensure** that the organisation's **personnel is aware** of the current strategy and policy and are familiar with the personnel's instructions.

2.2 Guideline for experts managing the use of artificial intelligence, information security, data protection and other support measures

1. **Provide instructions** on which applications, systems and services may or may not be used, why and within what limits they can be used.

2. **Ensure** that the use and development of AI, its guidelines, contract, licence terms and conditions are consistent with the organisation's strategy and policy as well as with legislation and other requirements.
   - Verify how AI supports statutory tasks and operates within allowed limits.
     - Take into consideration the changes to terms and conditions that will accompany service extensions, new modules, or versions.
   - When using artificial intelligence, take into account any copyright issues.
     - Consider the perspective of data entered and the owners of the data.
     - Consider the significance of the output and the teaching data contained in it.

3. **Take a risk-based approach to analysing** whether a matter or material can be processed using artificial intelligence or in a system that utilises artificial intelligence.
   - Take data protection and data classification into account. Instruct personnel on the use of permitted and prohibited materials. Classifications and metadata must be suitable for use with artificial intelligence.
   - Consider preparedness for the restrictions or the inability to use AI and also the need for its independent shutdown.

4. **Verify and agree** in writing the extent to which and under what conditions AI services may be utilised when subcontracting application development or other services.
   - Make sure that no data that is critical to the organisation's operations is leaked in connection with application development.
   - If artificial intelligence is utilised, agree on how its checks, testing, quality assurance and development monitoring will take place.
   - Find out about the liabilities for copyright risks in agreements.

5. Provide instructions and training to personnel on the principles related to AI, including:
   - Open and transparent use
   - Fairness, non-discrimination, and biases
   - Data protection and privacy
   - Security and reliability
   - Human-centred approach
   - Ethical planning and use
   - Continuous processing of user feedback and error information and deviation situations
   - Communication on the use of artificial intelligence
   - Participation and cooperation

6 **Take into account** the development of ethical guidelines and risk management related to the utilisation of AI and update the organisation's guidelines and processes accordingly.

7 **Network** with other organisations and stakeholders to engage in discussion. Share experiences, policies and receive and provide peer support.

8 **Communicate** regularly about current AI issues in a clear and inclusive manner internally and externally where necessary.

9 **Provide instructions** on how the recipients of the outputs should be informed of the use of artificial intelligence in the production of material (texts, images, videos and all other material produced with or utilised in the production of artificial intelligence).

10 **Assess the situation on a case-by-case basis** at the early stages of the use of artificial intelligence. Generally applicable instructions are modified as the experience progresses. The most essential is to collect information.

- Create a system to collect data on all AI-related incidents. Each AI system may be different and have specific characteristics to monitor, so ensure that you form an overall view.
- Consider the system's connection and consistency with information security incident reports, risk data, quality management, customer feedback, and software development in the way they are most effective to organise.

2.3 Guidelines for personnel

1 **Comply with** the organisation's operating principles (policy, guidelines, roles, processes) when testing, introducing, and using AI.

- Use AI applications only for purposes approved by the organisation.

2 **Use** only the AI applications approved by the organisation for data processing.

- If your software or online service reports that it has implemented use of AI-based features, notify the party in your organisation responsible for software approval.
- Check whether the service you are using is public AI service open to everyone or a service provided by your organisation and follow the instructions provided for its use.

3 **Do not assume that artificial intelligence is always correct.** Artificial intelligence is not infallible, and its decisions may be wrong. Do not rely blindly on its decisions or on the information it produces.

- Do not use AI-produced material (e.g. code, data, translations) if you do not understand what it does, contains and means.
- Review the data produced by artificial intelligence by other means, if possible.
- If you cannot or do not know how to check the accuracy of the information or other output produced by artificial intelligence, ask for help, do not publish, or make use of the information before it has been verified by another expert.

4 **If** artificial intelligence produces material that is of poor quality, incorrect, dangerous, or otherwise suspicious and inappropriate, stop using it. Document this by copying the texts, taking screenshots, or saving any error and log data for analysis.

- Report errors made by AI as agreed. Even minor errors can become a significant problem. Your organisation should provide instructions on how and what to report.

5 Whenever you use an AI application or service, **make sure** that you do not feed it materials restricted by the organisation.

- Examples of prohibited materials may include personal data, confidential information, classified information, copyrighted information, etc.

6 **If you are unsure**, ask your organisation's AI coordinator, information security expert, data protection officer or another expert.

- Give feedback to the AI coordinator and information security experts if you notice a loophole in the instructions, a feature that may hamper the reliable and secure functioning or reputation of your organisation or another defect.

7 **Keep** up to date, participate in related training and other events.

8 **Follow** the principles of good open administration and other official responsibilities – responsibility cannot be transferred to AI.

- As a rule, the content produced by AI must be reported in accordance with the organisation's guidelines.

9 See artificial intelligence as a positive, new support service that expands your competence.

2.4 Checklist for product owners, administrators and developers of AI-containing systems, service collections or processes

WHAT TO DO:

1 **Use** the AI services and resources provided to you by your employer in accordance with provided instructions to carry out work and implement planned projects.

- Experiments should be supported. However, they must be sufficiently limited, the risks must be assessed, and preparations must be made in advance for situations in which risks are realised.

2 Development measures and the use of artificial intelligence must **comply** with the organisation's strategy and policies. Any deviations from the policies and experiments must be processed in advance.

3 **Comply** with laws and regulations. Ensure that the use of AI to assist the operation of the system complies with all applicable laws and regulations, including data protection and non-discrimination laws. Regularly update your knowledge of their interpretation

and take a proactive approach to taking the main points of the EU AI Act (AIA)[1] into consideration in your system's features.

4 **Agree** with external consultants on how and within what limitations artificial intelligence can be utilised in development. Agree on quality management and accountability in writing.

5 **Take security into account** already at AI system's design stage, not just when deploying.

- Use reliable and tested systems. AI systems can be complex, so it is important to use well-designed and tested systems.
- Review how the system operates and its settings for security and data protection. Limit development and testing environments as required.
- Report any issues with the use of the system, identified threats, and observed risks associated in accordance with your organisation's instructions.
- Be prepared for potential problems. While AI systems are often reliable, it is important to prepare for potential problems or faults.
- Also pay attention to the possible end of the service's administration and sudden termination of the service. This may mean making contingency plans for alternative ways of accessing and processing data and fast communication.
- When using AI services, take care of all normal information security controls related to the use of services (e.g. service settings, password quality, MFA).

6 **Assess and ensure** the security of AI systems with thorough testing before introducing their use.

7 **Understand the limitations of AI**. Each AI system is designed for a specific purpose and has its own limitations. Identify the biased responses from the AI you are using. Understand these limitations and apply AI keeping them in mind.

8 **Design** the user experience of the AI system in a human-centred manner. Make sure it is easy to use and serves the needs of its users. An AI system should always serve people's needs, not the other way around.

9 **Ensure** that the solutions produced by the service are ethically acceptable, non-discriminatory and in compliance with data and privacy protection. Try to utilise the resources, checklists, standards, external audits as well as user and stakeholder comments available online.

10 **Consider** the impact of AI on employees. Artificial intelligence can change the dynamics of the workplace and the roles of employees. Try to identify these impacts in advance and plan changes carefully.

11 **Assess** what kind of risk arises if all the organisation's teaching data entered in the AI service are combined; will this aggregation create confidential or other data that may harm the organisation?

12 **Train** personnel to ensure that all employees have the knowledge and understanding of the capabilities and limitations needed for the safe use of the developed AI system.

13 **Inform** the user as clearly as possible if AI has been utilised when designing the system or the system uses AI to produce materials or process data (for what, why, what service, to what extent, etc.).

14 **Maintain** open communications. Whether it be an internal team or external stakeholders, open and continuous communication is key to the secure and efficient use of AI.

[1] AI Act | Shaping Europe’s digital future (europa.eu)

15 When using data produced or developed by the organisation itself as teaching data, **ensure** that it is of high quality and does not contain, for example, incorrect, obsolete results or other results that cause biases. The importance of testing is emphasised here, as well.

DO NOT:

16 **Do not use** artificial intelligence without purpose. It is just a tool that should always serve a clear purpose. Do not use AI simply because it is a new and interesting technology.

17 **Do not assume** that AI will solve (all) your problems. Artificial intelligence can help with many things, but it is not the solution to everything. Do not assume that AI can replace all other tools and processes.

18 **Do not forget** that there is a person behind artificial intelligence. Artificial intelligence systems are designed and implemented by people, so consider the resulting bias. Also note the person in front of the AI system, who interprets the system's operations and outputs. Taking the perspectives and objectives behind the system into account helps in this interpretation.

19 **Do not enter** any confidential, personal, or classified information in the service if you do not know whether the system has been approved for their processing. When using AI systems, "remembering" of the data must be taken into account, as must the possible use of the data to develop the system, in which case the data may be appear in other contexts.

- Do not enter data that you or your organisation does not have copyright for into a public service.
- Do not forget data protection. AI systems often use large amounts of data, and it is exceptionally important to protect and process these correctly.

20 **Do not forget** continuous monitoring. AI security is not a one-off event, but a continuous process that requires regular monitoring and updating.

21 **Do not ignore** user feedback. User feedback is a valuable resource for improving the security and efficiency of AI. Do not ignore their experiences and suggestions.

3. Checklist on questions related to the use of artificial intelligence

We have compiled a checklist below that allows the organisation to examine issues and needs related to the utilisation of AI. Some of them have been partly discussed earlier in this material.

1. Is the use of artificial intelligence in line with the organisation's strategy and goals?
- AI should support the company's overall strategy and objectives.

2. How does the organisation take a people-centred approach into account when designing services?
- Stakeholders and users related to the service are identified, considered and heard as part of developing the service and its lifecycle management.

3. Is there a clear need or problem that artificial intelligence can solve?
- AI should not be a solution for finding a problem but should resolve an existing need or problem. Common uses of AI include the automation of different work phases, with the aim of improving speed, efficiency, quality, or all of these.

4. Does the organisation have a clear understanding of how artificial intelligence works and how it should be managed?
- It is important to understand the principles of AI, and particularly the limitations of its operation. These also include contexts, information systems and platforms, as well as processes and services in which AI is used, because they affect expectations, interpretation, and requirements.

5. Have ethical and responsibility issues related to artificial intelligence been taken into account?
- These questions may be related to such things as discrimination, transparency, and data protection. In addition to immediate issues, the meanings of long-term and high scalability (volumes) should be considered, which means that even small issues can become significant.

6. How has the information security of the services been ensured?
- The security of AI services should be managed in the same way as all services provided or used by the organisation, supplemented by requirements specific to the uniqueness and diversity of AI services. Ensure that the AI service provider has ensured information security in its service. Even if the information is public, someone might want to influence the results or falsify the information. The assessment should be part of the risk assessment related to the development or implementation of the organisation's services, which also takes into account the risk and impact assessments required for the processing of personal data.

7. Identify regulation related to the whole
- Observe all applicable regulations and laws when using AI services. These may include EU or national regulations, data protection laws, industrial standards, and other rules. You will find examples of these later in this material. It is worth remembering

that, for example, the AI Act, which plays a significant role in the EU area, has just been approved in May 2024[2], and its implementation will take years.[3]

8. Figure out accountability issues in advance
- AI is not accountable for mistakes, people are. Always be prepared to take accountability for the decisions and actions of the AI system.

9. Ensure support for copyright and other legality-related issues
- Find out in advance what kind of copyright-related challenges are associated with sharing the information you produce and ensure that the necessary legal support is available in case of problems.

10. Have the obligations related to information management, the Act on the Openness of Government Activities and good governance been taken into account in the utilisation of artificial intelligence?
- When deploying services, a service compliance assessment must be carried out, one part of which is the fulfilment of legislative obligations. Also pay attention to the obligations that must be taken into account in the provision of AI services, which are often cloud services. Also recognise the possibility of using restricted, nationally produced AI services where necessary, of which the operation is based on, e.g., only the teaching data provided to the service.

11. Have the risks associated with the use of artificial intelligence been assessed and has a risk management plan been drawn up?
- The use of AI involves numerous risks, including technological risks, business risks and reputation-related risks. Have the risks been identified and how are they managed? And how has the possible realisation of these risks been taken into account in the continuity, preparedness and crisis communications plans?

12. Does the organisation have the resources and competence to deploy, maintain and train AI?
- The deployment and maintenance of artificial intelligence requires both technical and substance-related expertise and user training. The necessary user training for the use of AI services will be part of ICT user skills in the future. Similarly, a completely new type of competence development related to the special features of AI services will be needed for service developers.

13. How will the use of AI affect employees and customers?
- The use of artificial intelligence may involve social and cultural impacts, such as changes to work tasks and the very varied attitudes of customers towards artificial intelligence.

14. Does the organisation have a plan to assess and monitor AI usage?
- It is important to regularly assess the impacts of AI and make the necessary changes to its use. Indicators must be created in advance for effectiveness and other measurable matters, which are regularly measured, and activities are developed on the basis of these results.

[2] https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ - 21 May 2024
[3] https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf - 14 May 2024

15. How is the use of AI allowed in application development?
- What kind of policy does the organisation have for using AI in application development? This must be assessed regardless of whether the organisation develops applications itself. If the use of AI services is allowed in application development, what are the terms, restrictions, and controls that it requires? How will it be ensured that confidential data (including any algorithms) are not leaked to external actors?

16. How has the organisation updated the requirements related to the utilisation or use of AI into its procurement guidelines and requirements related to competitive tendering?
"The public procurement of services that produce or utilise AI services is still quite new, and many of the tasks already highlighted in this document must be considered in this context. As AI services operate on the "black box" principle, comparing services from different suppliers without the real user experience from written documentation alone can be challenging. The type of use the service is being acquired for will significantly affect the competitive tendering and the preparation of procurement requirements.

3.1 Please also note

1. **Artificial intelligence creates huge opportunities, but it also entails significant risks.** Cybercriminals, state-level actors and other parties will be able to use it more easily, with no regard for legislation or the ethics related to the activities. On the other hand, the same methods used to create these attacks can at least partly be used to defend ourselves from them.

2. The use of AI will significantly expand from what we now imagine it will be used for. For example, the use of the Internet network was considerably more limited in the 1990s, than in has been in 21st century due to the increased use of smart devices. The same can be expected for the utilisation of artificial intelligence. If it took ten years for a technological service or phenomenon to become more common in the 1990s or early 2000s, a similar leap can now be made in a much shorter time, within a few years or depending on the case in question even months. This is due to the significant i.e. exponential development of technological performance annually.

3. AI results in **many benefits**, but it also **consumes resources and increases risks**. Sufficient usefulness, responsibility and risk assessments must be carried out before starting its use. The responsible use of AI also takes into consideration whether the use of AI is proportionate in all use cases. According to the IEA report, the electricity consumption of data centres, artificial intelligence and the crypto-currency sector may double by 2026 [4].

4. When assessing the risk level, the safest way to experiment with artificial intelligence is when success creates a great deal of positive or is really useful, but failure will not cause much harm. If the technical and administrative implementation of artificial intelligence (e.g. neural network) forms a "black box" that is difficult to manage and understand, the risks must be managed in the process before it (correct

[4] https://www.iea.org/reports/electricity-2024/executive-summary

targeting, data, and its quality) and after it (output control, filtering and effective error correction and learning).

5. Artificial intelligence **does not have a plan or aim to achieve the right result**; a path to conclusions that has begun incorrectly can only lead to increasingly worse results.

6. **Artificial intelligence provides a statistically correct answer**, not the correct answer; the answer it produces is as good or bad as the data used in its teaching. This also applies to teaching data produced by the organisation itself, using it does not automatically guarantee the correct outcomes but will depend on such things as the accuracy and timeliness of the data.

7. Artificial intelligence is **effective in producing answers**, which means that **mistakes are duplicated quickly,** and this must be taken into consideration when developing a service or process that utilises artificial intelligence. This requires the simultaneous development of adequately efficient and scalable means of correcting and managing errors. These also include a clear practice for halting the use of AI, but this does not yet resolve the minimisation and correction of potential damage caused.

8. In the future, the manipulation of teaching data will be a growing risk, so the quality of the information produced by AI must be monitored.