Questionnaire for AI companies in Europe

Contents

Part 1: Basics	4 questions
Part 2: Data storage	5 questions
Part 3: AI Development	8 questions
Part 4: AI Security	3 questions
Part 5: AI Regulations (present and future)	9 questions
Part 6: AI Ethics	7 questions

Procedure

1) I will show you the question
2) I will show you the answer options (if they exist)
3) You will have time to choose an answer and give me more feedback if you want (I will write down your answers separately, you do not have to click on anything)

Approximate time: 45 minutes

Part 1: Basics

4 questions

1) How old are you?

Open question

2) How many years of experience do you have in developing AI systems?

Open question

3) Does your AI leverage Deep learning (i.e. neural networks)?

❏ Yes

❏ No

4) Does your AI - or part of it - qualify as “high-risk” (as proposed by the EU)?

❏ Yes

❏ No

❏ I don’t know

Which AIs are considered high-risk?

AI systems identified as high-risk include AI technology used in:

- critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
- educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- safety components of products (e.g. AI application in robot-assisted surgery);
- employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures);
- essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan);
- law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
- migration, asylum and border control management (e.g. verification of authenticity of travel documents);
- administration of justice and democratic processes (e.g. applying the law to a concrete set of facts).

Part 2: Data Storage

5 questions

1) Is the data you use for the development / improvement / use of your AI stored within Europe, or do you store it elsewhere?

❏ Europe

❏ Elsewhere (please specify)

2) Which, if any, cloud provider do you use for AI development? (e.g. AWS Cloud AI Developer Services, Google Cloud, etc.)

Open question

3) Do you think that some countries outside of Europe have a regulation landscape that would make your business more profitable or favourable (e.g. USA, China)?

❏ Yes

❏ No

4) If your data is currently stored outside of the EU, how difficult would it be for you to relocate your data to a local data storage (within Europe)?

1: Very easy

10: Very difficult

5) If the answer to the previous question is above 5: Why is it very difficult to relocate your data?

Open question

Part 3: AI Development

8 questions

1) How often do you assess the performance of your AI?

❏ Daily

❏ Weekly

❏ Monthly

❏ Quarterly

❏ Semi-annually

❏ Yearly

❏ Never

2) How do you ensure that the AI system will maintain an adequate level of performance over-time?

❏ Retrain AI in regular frequencies (with new data)
❏ Alert system if accuracy declines
❏ We do not have any performance checks in place at the moment
❏ Other: Please explain

3) Accountability in AI is becoming increasingly important. Do you already have systems in place that oversee accountability?

Accountability: Mechanisms to ensure responsibility, accountability, and auditability for AI systems and their outcomes

❏ Yes

❏ No

❏ No, but plan to do so soon

4) What do you consider more important: The explainability or the accuracy of your AI?

Explainability: AI that "allows human users to comprehend and trust the results and output created by machine learning algorithms" - IBM

❏ Explainability

❏ Accuracy

❏ We choose a trade-off between explainability and accuracy

5) Bias in AI can occur in many different ways (imbalanced data collection, wrongly labelled samples, biased engineers, etc) and prevents the AI from working correctly. Have you thought of measures on how to mitigate bias?

❏ Yes

❏ No

❏ No, but plan to do so soon

6) If yes, what have you implemented?

Open question

7) Which of the following is accessible to the public:

- ❏ Training Data
- ❏ Test/Evaluation Data
- ❏ Model (for example via API)
- ❏ None

8) Which of the following is accessible to your <u>client</u>:

❑ Training Data

❑ Test/Evaluation Data

❑ Model (for example via API)

❑ None

Part 4: AI Security

3 questions

1) Do you consider security-by-design principles when developing your AI?

❏ Yes

❏ No

❏ No, but plan to do so soon

Examples for security-by-design principles on the next slide

Examples for Security-by-Design by OWASP:

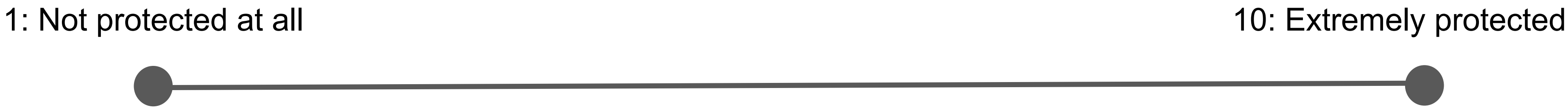
1. Minimise attack surface area
2. Establish secure defaults
3. The principle of Least privilege
4. The principle of Defence in depth
5. Fail securely
6. Don’t trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

2) Are you aware that the intellectual property of your AI might be at risk? (somebody stealing your AI)

❑ Yes

❑ No

3) How well protected is the intellectual property of your AI?



1: Not protected at all

10: Extremely protected

Part 5: AI Regulations in Europe

9 questions

1) How often do you encounter legal issues with your AI?

❑ Never

❑ Sometimes (please explain)

❑ Often (please explain)

2) There are calls for more policies and regulations to clarify what is allowed and what isn’t in the field of AI. Would you prefer more ‘fine-grained’ regulations or more general ones?

More fine-grained could mean that it is explicitly stated which AI systems in which industries fall under which rules so that you are clearly informed what you as a company is allowed to do so you don’t have to worry about getting sued.

❏ More fine-grained

❏ More general

❏ No preference

3) Do you regularly consult with an expert/lawyer about the current regulations affecting the use of AI?

❏ Yes

❏ No

❏ No, but plan to do so soon

❏ Want to do so, but do not know who is expert in this field

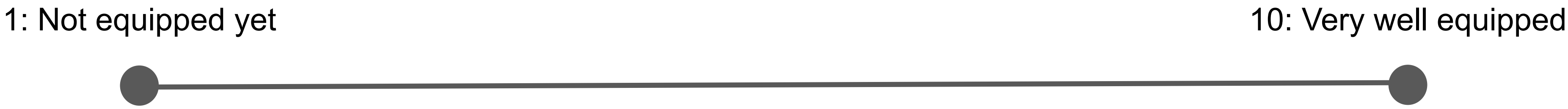
4) Some existing regulations state that businesses must remove potentially a large amount of data due to privacy protection reasons. Additionally, users could renounce businesses the right to use their data for certain purposes. Do you have fine-grained access to your training data to remove one specific sample?

❏ Yes

❏ No

❏ No, but soon

5) How well equipped is your business to react to many (e.g. all of a sudden 50 a day) unforeseen requests to remove samples?



1: Not equipped yet

10: Very well equipped

6) Do you think that, when asked about disclosing documentation by legal authorities, you must disclose more information than what you currently have available?

- ❏ Yes, we will need to disclose more information than we currently have available
- ❏ No, we have enough documentation available
- ❏ We have not thought about this yet

7) Future regulation might require AI businesses to disclose to users that they are currently interacting with an AI. Do you already disclose that information to the end-users of your product?

❏ Yes

❏ No

❏ No, but plan to do so soon

❏ Our AI does not interact with end-users directly

8) Do you think that regulations compliance and cyber security measures only harm your AI business or have you thought about using it as an opportunity?

❏ Regulations and security harm my business

❏ We use security and compliance to add value to our business

❏ We have never thought about this

9) What do you think should be done to improve the current regulations landscape?

Open question

Part 6: AI Ethics

7 questions

1) Research found that most people consuming AI products are incapable of understanding what it is and what it does. Do you think informing your clients about the general architecture of your AI improves trustworthiness? (Not the explainability of the output)

❏ Yes

❏ No

2) If yes, how feasible would it be in your case to explain what your AI does (its architecture and how it works)?

1: Not feasible, too complicated

10: Feasible, can explain

3) From 1 to 10, how much would your company benefit if the general population had a better understanding of AI?

1: Not benefit at all

10: Benefit a lot

4) The Assessment List for Trustworthy Artificial Intelligence (ALTAI) is a checklist created in 2020 by a high-level expert group on artificial intelligence appointed by the European Commission. Have you heard about it?

❏ Yes

❏ No

5) The expert group has created 7 areas of AI where businesses can ensure the trustworthiness of their AI. Which of the following KPI's are you already implementing?

- ❏ **Human agency and oversight:** AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights
- ❏ **Technical robustness and safety:** AI systems need to be resilient and secure and ensure a fall back plan in case something goes wrong
- ❏ **Privacy and data governance:** Besides ensuring full respect for privacy and data protection, data governance mechanisms like quality and integrity of the data, and legitimised access to data should be ensured
- ❏ **Transparency:** The data, system and AI business models should be transparent (traceability mechanisms) and humans need to be aware that they are interacting with an AI system
- ❏ **Diversity, non-discrimination and fairness:** Unfair bias must be avoided
- ❏ **Environmental and societal well-being**: AI systems should benefit all human beings, including future generations
- ❏ **Accountability**: Mechanisms should be put in place to ensure responsibility, accountability, and auditability for AI systems and their outcomes
- ❏ **None of the above**

6) If you haven’t already applied measures, would this checklist help you in making your AI more trustworthy in the future?

❑ Yes

❑ No

❑ Not sure

Thank you for your participation!