Revealing the European Practitioners' viewpoint on the AI Act

Appendix Q Questionnaire: Explanations and Motivations

In this appendix, we provide an extended description of our questionnaire (discussed in §3.1.2 of our main paper). Our intention is explaining the reasons that moved us to formulate the 36 questions that we asked during our semi-structured interviews.

Q.0 Overview

The questionnaire consists out of six parts: basics, data storage, AI development, AI security, AI regulations (present and future), and AI ethics. These sections were derived from the plethora of topics from current research and other relevant contemporary AI topics. Each section provides insight into their respective field:

1. Basics: Demographic insights about the interviewee and general information about their AI (whether it leverages deep learning and whether it is considered risky by the AI Act)
2. Data storage: Where the companies store their data for the development, improvement, and use of their AI and how easy it would be for them to relocate their data. Additionally, information about which cloud providers are used to develop AI.
3. AI security: Where companies put the focus on during the development of their AI in regards to accuracy or explainability and how bias is prevented, if at all.
4. AI regulations (present and future): This section asks questions about security-by-design principles and intellectual property.
5. AI ethics: Insights into how transparent companies are about their AI and whether and how they invested into the trustworthiness of their system.

The questions are explained on the following pages, including which question they are intended to answer and which findings by the research body sparked the question.

Q.1 Basics

Q1.1 How old are you? *Open question*

This question is for demographics to group the interviewees into different age groups. It could be interesting to assess whether different age groups give different answers. Additionally, this question can be used to assess whether this interview study is representative and comparable to similar studies in terms of the age of the interviewees.

Q1.2 How many years of experience do you have in developing AI systems? *Open question*

This question is for demographics. Asking about work experience can help assess a cand-idate's qualifications and skill level. Additionally, similar to Q1.1, this question can be used to assess whether this interview study is representative and comparable to similar studies in terms of the experience of the interviewees.

Q1.3 Does your AI leverage Deep learning (i.e. neural networks)? *Yes / No*

Differentiating whether an AI company uses deep learning or not is important because it can provide valuable insights into the company's capabilities, limitations, and potential applications. Deep learning is a subfield of machine learning that has gained increasing attention due to its ability to learn and improve from data, and it has shown remarkable success in various applications, such as image and speech recognition, natural language processing, and autonomous driving (Heaton, 2017; LeCun et al., 2015).

Q1.4 Does your AI - or part of it - qualify as "high-risk" (as proposed by the EU)?
Yes / No / I don't know

It is important to ask whether a company qualifies as "high-risk" as proposed by the European Commission in the AI Act because it can have significant implications for the development, deployment, and regulation of AI systems. The AI Act proposes a risk-based approach to AI regulation, where higher-risk AI systems are subject to more stringent requirements and oversight to ensure their safety, transparency, and accountability (*Artificial Intelligence Act*, 2021). By knowing whether a company's AI system falls under the high-risk category, one can better understand the potential risks and benefits of the system, the legal and ethical implications of its use, and the need for compliance with the regulatory framework. Furthermore, identifying high-risk AI systems can also help prioritize resources and efforts for testing, certification, and monitoring to ensure their compliance with the legal requirements and prevent harm to users and society at large (Hagendorff, 2020). Therefore, asking whether a company qualifies as "high-risk" under the AI Act can provide valuable information for evaluating the company's ethical and social responsibility and for promoting trustworthy and human-centric AI.

Q.2 Data Storage

Q2.1 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)

The GDPR requires personal data used by a company needs to be stored within the European Union or an outside place that offers the same level of data protection ("General Data Protection Regulation - GDPR", 2018). This question therefore should identify whether companies are already storing their data in Europe or not.

It is important to know where European AI companies store the data for the development of their AI system because it can have implications for data protection, privacy, and security. The General Data Protection Regulation (GDPR) requires companies that collect and process personal data of European citizens to comply with strict standards for data protection and security ("General Data Protection Regulation - GDPR", 2018). Therefore, knowing where the data is stored can help determine whether the company is complying with the GDPR and whether the data is subject to adequate protection and safeguards against unauthorized access, disclosure, or misuse. Therefore, asking about the location of data storage can provide valuable information for evaluating the trustworthiness and responsibility of European AI companies.

Q2.2 Which, if any, cloud provider do you use for AI development? (e.g. AWS Cloud AI Developer Services, Google Cloud, etc.)
Open question

This question is important because certain cloud providers use storage options outside of Europe to provide their solutions. In this case, it might be of importance for AI companies to double-check whether their choice of cloud storage is GDPR-compliant (Barati et al., 2022). This question attempts to raise awareness about this topic. Additionally, this question gives insight into which systems and providers the AI companies use for AI development.

Q2.3 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

A potential problem correlating with AI regulation in Europe is that it could drive companies out of the European market. The European regulations including GDPR and now the AI Act could make AI companies relocate to a different market like the US or China because it is easier to follow the restrictions there (Glauner, 2022, pp. 6). Additionally, Liebl and Klein (2022) found that some AI companies are - in fact - considering to relocate outside of the EU because the AI Act might make working on their system too hard. This would be problematic for the European Union as their goal with the AI act is to "provide key competitive advantages to companies and the European economy" (*Artificial Intelligence Act*, 2021, pp. 1). There is a potential risk that the AI Act has the opposite effect on

European AI companies. This question aims to identify whether this might be the case.

Q2.4 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

Q2.5 If the answer to the previous question is above 5: Why is it very difficult to relocate your data?
Open question

This question shall identify how difficult it would be for a company to relocate their data if their data is currently stored outside of Europe. The GDPR requires personal data to be stored within the EU, therefore if a company does not yet fulfill such a standard, this question identifies how difficult it would be ("General Data Protection Regulation - GDPR", 2018). Additionally, in the case a company stores it data outside of Europe and finds it extremely difficult to relocate the data, finding out the reasons for that would provide valuable insights.

Q.3 AI Development

Q3.1 How often do you assess the performance of your AI?
Daily / Weekly / Monthly / Quarterly / Semi-annually / Yearly / Never

Q3.2 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 (Multiple answers possible here)

The AI Act might require AI companies to apply adequate quality management to their applications (*Artificial Intelligence Act*, 2021, pp. 31). Additionally, research has shown that it is not sufficient to simply assume an AI will produce the same quality of output without supervision once it is deployed: "some processes start out achieving desired outcomes and then change unexpectedly at some point" (Larson & Boland, 2019). The above two questions should therefore identify how regularly companies assess the performance of their AI and what they implement. The outcome will show whether companies are already complying with the idea of adequate quality management or whether there is still room for improvement.

Q3.3 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

According to the AI Act, especially high-risk AI systems will need accountability frameworks that clearly denote the responsibilities of the staff working on the system (*Artificial Intelligence Act*, 2021, pp. 54). Additionally, the GDPR states the "right to explanation" in Articles 13-15 ("General Data Protection Regulation - GDPR", 2018). This would be applicable for AI systems that process personal data and means that a person who's data is used for the development and use of the AI system could require the AI company to reveal how the AI system works - to explain. Furthermore, aside from regulation efforts, Busuioc (2021) and Doshi-Velez et al. (2017) discuss how accountability in automated systems is important in order to assign who is responsible for potential harm caused by these systems. This question should identify whether AI companies have already put mechanisms into place that define who worked on what part of the AI system.

Q3.4 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

Explainable AI applications allow "humans to understand, appropriately trust, and effectively manage" them (Barredo Arrieta et al., 2020, pp. 83). In the future it is to be expected that AI applications which output is possible to be explained are going to be trusted more. Additionally, with the AI application being explainable, potential bias can also be reduced or eliminated (Gade et al., 2019). Model explainability can be used as a means of trust and might be an important topic in the future of AI development in Europe. Therefore, this question aims to find out what the current status in the industry of AI companies is like: Do they focus on pure performance (accuracy) or are they also concerned about the explainability of the results?

Q3.5 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

Q3.6 If yes, what have you implemented?
Open question

As already touched upon in the question above, bias is an important topic in AI development because while AI can aid in keeping systems objective, AI "can also bake in and scale bias" (Silberg & Manyika, 2019, pp. 2). Evidence has shown that AI models can take over human bias if not closely monitored (Silberg & Manyika, 2019). This question identifies whether AI companies are aware of the existence of bias and whether they have any measures in place already to mitigate bias.

Q.4 AI Security

Q4.1 Do you consider security-by-design principles when developing your AI?
Yes / No / No, but plan to do so soon

AI companies are highly likely to be exposed to cyber threats which can distort not only the sample, but also the system learning and the decisions (Li, 2018). It is therefore important for companies to be appropriately secured against such threats. This question aims to find out the general awareness and adoption of cyber security in regards to AI systems.

Q4.2 Are you aware that the intellectual property of your AI might be at risk? (somebody stealing your AI)
Yes / No

Q4.3 How well protected is the intellectual property of your AI?
1: Not protected at all / 10: Extremely protected

The field of Artificial Intelligence is relatively new to copyright protection. Abbott (2017) even goes as far to say that Intellectual Property (IP) law is not properly prepared for this step. Questions that bother the community are who is given the IP, the machine or its creators (Kurian, 2021)? Nevertheless, if these systems are not given proper protection, they might be at risk of being "stolen": Somebody could take the same idea, the same system, and monetize it for themselves. This question aims to find out whether AI companies are aware of this potential situation.

Q.5 AI Regulations

Q5.1 How often do you encounter legal issues with your AI?
Never / Sometimes (please explain) / Often (please explain)

This question is supposed to give insights into how many companies encounter legal issues at what rates. Especially small companies are under more pressure because they might not have the educated staff to tackle certain legal questions (Bessen et al., 2020).

Q5.2 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

This question is supposed to offer insight into whether companies prefer fine-grained over general regulations regarding AI. As also noted by Dr. Philipp Hacker (2020), horizontal regulation that is not too specific and tries to cover all use cases might be adequate also for AI. However, what do companies, especially small companies think about this? It will be useful to see whether they rather work with general regulations where they can potentially work around certain rules, or whether they rather know exactly what is allowed and what is not.

Q5.3 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

As regulations in the field of data processing and AI are still new (GDPR came in 2018), there might not be enough experts in this field to consult AI companies. Research also shows that companies in Europe are likely to create entire positions that handle GDPR-related topics (Bessen et al., 2020). If there are a lot of companies who would want and need professional advice but cannot find a suitable lawyer, this would show a general need for more experts in this field.

Q5.4 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

Q5.5 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

The "right to be forgotten" is stated in the GDPR ("General Data Protection Regulation - GDPR", 2018). It means that a person can withdraw their consent that their data is allowed to be used for a certain purpose. Therefore, an AI system that is using personal data needs to be prepared that a person might make use of their right to be forgotten. These questions therefore aim to find out whether companies are already ready to do so.

Q5.6 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

This question aims to find out how well documented the AI systems of the companies already are. The AI Act might require certain AI systems to be well documented *Artificial Intelligence Act* (2021). In case of an audit, companies might need to provide documentation about their AI systems. Additionally, documentation is not only necessary for audit processes, but should also be of interest to the AI company in general, since it allows to identify how the outcome of the system came about. Felzmann et al. (2020) says that all parts involved in the development of the AI system "should be documented to the best possible standard" (Felzmann et al., 2020, pp. 3347). This question should therefore determine how well documented AI companies already are without having regulatory pressure.

Q5.7 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

Transparency requirements according to the AI Act will apply to all AI systems interacting with humans, detect emotions or generate deep fakes (*Artificial Intelligence Act*, 2021, pp. 14). Therefore, it is relevant to ask whether AI companies currently already disclose to end-users that they are interacting with an AI. This question only applies to AI systems interacting with people directly.

Q5.8 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

This question is supposed to shine light on whether AI companies in Europe are feeling like they are held back by regulations and cyber security measures. If the majority feels like cyber security measures and regulations stop them from being successful, it would an important message to lawmakers in Europe.

Q5.9 What do you think should be done to improve the current regulations landscape?
Open question

This question gives the interviewees the opportunity to give any information into what they would improve in the current regulations landscape. Therefore, this question should cover anything about regulations and AI that the previous questions have not been able to.

Q.6 AI Ethics

Q6.1 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

Q6.2 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

Santiago (2019) found that individuals still trust AI systems, even if said systems are proven to produce false outputs. This question aims to find out whether AI practitioners believe whether their clients would

trust their AI systems more if they knew about it. Through such informing, individuals could potentially make better informed decisions, therefore mitigating the effect explained by (Santiago, 2019). Additionally, the questions aim to find out how easy it would be to explain how the AI systems of the practitionres work.

Q6.3 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

As stated in the question above, research suggests that business leaders have a tendency to blindly trust AI systems, even when certain systems are proven to be faulty (Santiago, 2019, pp. 189). The question arises whether AI business potentially use this research outcome to boost their products, since blind trust in AI is high. The above three questions therefore aim to find out whether AI companies believe that more knowledge about AI helps them or rather causes problems to them. If companies believe that a knowledgeable client base and general public might lead to less sales, it could indicate that these AI businesses use AI more as a marketing term.

Q6.4 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

Q6.5 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

Q6.6 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

The Assessment List for Trustworthy Artificial Intelligence (ALTAI) was created by a high-level expert group on AI by the European Commission (European Commission, 2020). This checklist is not mandatory to any AI businesses in Europe and can be used to create ethical AI systems. Additionally, as Thiebes et al. (2021) states, the benefits of AI are maximised when AI is built with trustworthiness and ethics as a basis. The above questions shall identify where AI companies stand in regards to AI ethics. Even if they do not know the ALTAI list, the questions should find out whether they already implemented systems to ensure trustworthiness. Moreover, if a lot of companies already fulfill most of the above points in the assessment list, one could argue that it is not necessary to even regulate the field at all. Companies can use ethics and trustworthiness as leverage over others, which then would automatically regulate the AI market on its own.

References

Abbott, R. B. (2017). Artificial intelligence, big data and intellectual property: Protecting computer-generated works in the united kingdom. *Intellectual Property: Patent Law eJournal*.

Artificial intelligence act (tech. rep.). (2021). European Commission.

Barati, M., Aujla, G. S., Llanos, J. T., Duodu, K. A., Rana, O. F., Carr, M., & Ranjan, R. (2022). Privacy-aware cloud auditing for gdpr compliance verification in online healthcare. *IEEE Transactions on Industrial Informatics*, *18*(7), 4808–4819. https://doi.org/10.1109/TII.2021.3100152

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai. *Information Fusion*, *58*, 82–115. https://doi.org/https://doi.org/10.1016/j.inffus.2019.12.012

Bessen, J., Impink, S., Reichensperger, L., & Seamans, R. (2020). Gdpr and the importance of data to ai startups. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3576714

Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review*, *81*(5), 825–836.

Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., Scott, K., Schieber, S., Waldo, J., Weinberger, D., et al. (2017). Accountability of ai under the law: The role of explanation. *arXiv preprint arXiv:1711.01134*.

Dr. Philipp Hacker, L. (2020). AI Regulation in Europe. *Science*, *40*(40), 122–5.

European Commission. (2020). *Assessment List for Trustworthy Artificial Intelligence (ALTAI)*.

Felzmann, H., Fosch Villaronga, E., Lutz, C., & Tamò Larrieux, A. (2020). Towards transparency by design for artificial intelligence. *Science and Engineering Ethics*, *26*. https://doi.org/10.1007/s11948-020-00276-4

Gade, K., Geyik, S. C., Kenthapadi, K., Mithal, V., & Taly, A. (2019). Explainable ai in industry. *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 3203–3204. https://doi.org/10.1145/3292500.3332281

General data protection regulation - gdpr. (2018, May 23). European Commission. https://gdpr-info.eu/

Glauner, P. (2022). An assessment of the ai regulation proposed by the european commission. https://doi.org/10.1007/978-3-030-99838-7_7

Hagendorff, T. (2020). The ethics of ai ethics: An evaluation of guidelines. *Minds and Machines*, *30*. https://doi.org/10.1007/s11023-020-09517-8

Heaton, J. (2017). Ian goodfellow, yoshua bengio, and aaron courville: Deep learning: The mit press, 2016, 800 pp, isbn: 0262035618. *Genetic Programming and Evolvable Machines*, *19*. https://doi.org/10.1007/s10710-017-9314-z

Kurian, N. R. (2021). Granting intellectual property rights to robots: Invitation of an ai apocalypse or evolution of a new legal system? *INTELLECTUALIS*, 21.

Larson, D. B., & Boland, G. W. (2019). Imaging quality control in the era of artificial intelligence [Special Issue: Quality and Data Science]. *Journal of the American College of Radiology*, *16*(9, Part B), 1259–1266. https://doi.org/https://doi.org/10.1016/j.jacr.2019.05.048

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*, 436–44. https://doi.org/10.1038/nature14539

Li, J.-h. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology and Electronic Engineering*, *1*(19).

Liebl, A., & Klein, T. (2022). AI Act impact survey.

Santiago, T. (2019). Ai bias: How does ai influence the executive function of business leaders? *Muma Business Review*, *3*, 181–192. https://doi.org/10.28945/4380

Silberg, J., & Manyika, J. (2019). Notes from the ai frontier: Tackling bias in ai (and in humans). *McKinsey Global Institute*, *1*(6).

Thiebes, S., Lins, S., & Sunyaev, A. (2021). Trustworthy Artificial Intelligence. *Electronic Markets*, *31*(2), 447–464.