VISCHER

CHECKLIST ON AI FOR CONTRACTS WITH SUPPLIERS & PARTNERS

David Rosenthal

Project/Provider: _____ Assessed: _____

Requirement (★ = key)	Data Protection	Secrecy	Copyright	AI Regulation	General	Assessment of the project/provider
Identification of AI The supplier's or partner's use of artificial intelligence (AI) in its services, products or activities has been identified, and there is an obligation to identify such use once it happens. In short, AI can be understood as any automated system, that is designed to operate with a certain level of autonomy (i.e. that has also been "trained" instead of only being programmed).				✓	✓	☐ OK ☐ NOK ☐ N/A
Data Processing Agreement ★ Where the supplier or partner acts as a processor, there is a data processing agreement in place that satisfies the requirements of applicable data protection law, such as the GDPR and Swiss DPA.	✓					☐ OK ☐ NOK ☐ N/A
Data Sharing/Joint Controller Agreement Where the supplier or partner acts as a sole or joint controller, the responsibilities of the supplier and partner as well as the customer have been defined, including any warranties with regard to (personal) data shared or collected, and restrictions in its processing by either party.	✓	✓			✓	☐ OK ☐ NOK ☐ N/A
Use of Data by Provider Restricted ★ The supplier's or partner's right to use customer's data and other data obtained from or for the customer in connection with the services, products and activities for training of their own AI models and other secondary use has been expressly disclaimed or otherwise regulated, in line with what the customer is ready and allowed to permit. As a standard, no AI training or other secondary use should be permitted, except where necessary for the services, products or activities. Where such training or other secondary use occurs on an "anonymized" basis only, the standards for anonymization and validation of its effectiveness should be agreed. Where data is used for training, protections against "data leaking" from the resulting AI models and compliance with data subject rights (including the withdrawal of consent, where relevant) should be regulated.	✓	✓	✓			☐ OK ☐ NOK ☐ N/A
Deletion Obligation Following the termination of the contract, the supplier or partner shall have the customer's data (even if not personal data) permanently deleted	✓	✓	✓			☐ OK ☐ NOK ☐ N/A

without retaining a copy, except where required by law, or where deletion is not reasonably possible (e.g., backups), in which case such data shall continue to be treated as confidential.						
Cross-Border Transfer Safeguarded ★ Any transfer of personal data (including through remote access) to the supplier or partner or to their subcontractors or other third parties involved is in compliance with rules for cross-border transfers of such data, namely that personal data can only be transferred to countries with the proper adequacy decision or contractual safeguards (e.g., EU SCC, with country specific amendments, as necessary). Where necessary, a transfer impact assessment (TIA) has been made with a successful outcome.	✓					☐ OK ☐ NOK ☐ N/A
No Sale of Data to Third-Parties ★ The customer's data and other data gained by supplier or partner from or for the customer in connection with the services, products and activities shall not be sold or otherwise made available to third parties, except where and to the extent expressly agreed with the customer in each instance.	✓	✓	✓			☐ OK ☐ NOK ☐ N/A
Adequate Information Security ★ The supplier or partner undertakes to provide for technical and organizational measures to ensure an adequate level of information security with regard to its services, products and activities. They shall take into account the specific means that can be used to attack an AI system, e.g., by way of prompt injections/jailbreaking, poisoning and sponge attacks.	✓	✓	✓	✓	✓	☐ OK ☐ NOK ☐ N/A
Rights of Affected Persons The parties have agreed on how to handle legitimate requests of persons affected by the processing of their personal data or the use of AI (even if no personal data is at issue). This may include the supplier or provider being required to provide for certain features in connection with its services, products and activities that enable the customer to delete, block or search and access the data of such persons (e.g., filtering of AI input and output for occurrences of certain personal data or third party content).	✓		✓	✓		☐ OK ☐ NOK ☐ N/A
Confidentiality Obligation ★ The supplier or partner shall itself and shall, by way of written declarations, have its personnel and subcontractors keep confidential any customer data and protect it with technical and organizational means of information security commensurate to the sensitivity of the data and risk involved in its processing. Where professional or official secrecy is at issue, this shall be expressly referenced. The obligation to keep data confidential shall last for as long as applicable law requires or there is a legitimate interest of the customer (or affected third parties) in the data being kept confidential. As part of the confidentiality obligation, the supplier or partner should also undertake not to use customer data for purposes other than the performance of the contract.		✓	✓			☐ OK ☐ NOK ☐ N/A
"Defend-your-Data" Clause		✓				☐ OK

The supplier or partner shall, if confronted with an attempt by a public authority or other third party to access customer data or request its production (i) inform the customer and direct the third party to the customer (where permitted) and (ii) unless instructed otherwise by the customer in any event use all legal means to object to such access or production (including on the basis that it violates the laws of the customer), or, if not possible, limit the scope of it and obtain all available protections.						☐ NOK ☐ N/A
Restriction on Operator Access The personnel of supplier or partner (or its subcontractors) shall only access customer data if either permitted by customer in each instance ("access approval") or where mandated by a binding enforceable order (or law applicable [to the customer]). Exceptions may apply where the service, product or activities, by their nature, require human operator access.		✓				☐ OK ☐ NOK ☐ N/A
Data Localization The supplier or partner shall store [and process] customer data exclusively in the geographical regions agreed with the customer[, including for the purposes of customer support, security operations and abuse control]. Data localization may be available only for certain services.	✓	✓				☐ OK ☐ NOK ☐ N/A
Compliance with AI Regulations The supplier's or partner's services, products or activities shall be in compliance with AI regulations applicable to both the supplier or partner, and the customer, including [in any event/if applicable] the EU AI Act. This includes having determined and agreed on the respective regulatory "roles" of the supplier or partner and the customer (provider, deployer, importer, etc.).				✓		☐ OK ☐ NOK ☐ N/A
AI Regulations Compliance Support The supplier or partner shall provide the customer with any reasonably requested support to enable the customer to comply with its own obligations under applicable AI regulations, including providing the necessary documentation and responses to questions.				✓		☐ OK ☐ NOK ☐ N/A
No Prohibited Use of AI The supplier's or partner's services, products or activities, if used as intended, are not prohibited under the AI regulations applicable to the supplier or partner and the customer.				✓		☐ OK ☐ NOK ☐ N/A
Use of Watermarks The parties have agreed whether and how the output generated by the supplier's or partner's services, products or activities shall be watermarked or otherwise marked as required by law, in particular where they have been generated or modified by AI.			✓	✓		☐ OK ☐ NOK ☐ N/A
Monitoring, Incident Reporting The supplier or partner shall permanently track incidents concerning its services, products and activities (including those happening to other users), and shall report to the customer any developments that may indicate problematic AI behavior or AI use or otherwise be relevant with regard to the reliability, safety, security and compliance of its services, products and activities.				✓	✓	☐ OK ☐ NOK ☐ N/A

De-Biasing The supplier or partner shall have the AI models used for or by its services, products and activities trained, fine-tuned or otherwise controlled to reasonably ensure that the AI outputs generated do not show unwanted bias. It has tested these services, products and activities accordingly.	✓			✓		☐ OK ☐ NOK ☐ N/A
Audit-Trails / Logging The supplier or partner shall enable the customer to fully document, by way of logs, the input, the output and other use of its services, products or activities. Such logs shall be immutable and occur at a user level. The customer must be allowed to retain them for at least one year.	✓			✓	✓	☐ OK ☐ NOK ☐ N/A
Compliance of AI Model Training The supplier or partner undertakes and warrants that the AI model(s) used by its services, products and activities has or have been trained in compliance with applicable law, whereby the parties have agreed whether such laws also include the laws applicable to the customer or certain other jurisdictions and, in the case of general purpose AI models under the AI Act, EU copyright law. If the services, products and activities include training or fine-tuning, such obligations shall apply accordingly.	✓		✓	✓	✓	☐ OK ☐ NOK ☐ N/A
Instructions of Use and Support The supplier or partner provides the customer with adequate instructions, training and support, on how to properly use the services or products supplied, or activities undertaken by it, and how to handle problems that may arise. The instructions shall also disclose any known issues and risks to be reasonably considered.				✓	✓	☐ OK ☐ NOK ☐ N/A
Tested AI The supplier or partner undertakes and warrants that it has properly tested, or will properly test, the services, products and activities for their compliance with the requirements before permitting productive use. Such testing shall be documented, with the documentation being available to the customer.	✓			✓	✓	☐ OK ☐ NOK ☐ N/A
Explainability The supplier or partner shall provide the customer with the necessary documentation and other information to permit the customer to reasonably understand (i) how the AI components used in or by the services, products and activities work and (ii) why, in principle, the AI has generated the output or made the decision it has made (which requires an understanding of the basic logic of the AI and the data it relies upon when applying it).	✓			✓	✓	☐ OK ☐ NOK ☐ N/A
Human Oversight The supplier or partner undertakes and warrants that the AI components of its services and products have the features necessary to enable the customer to maintain human oversight. Where the supplier or partner itself applies AI for its activities, it undertakes to itself implement human oversight to any use of AI that may have relevant negative consequences for third parties (including the customer), and have these humans intervene where necessary.	✓			✓	✓	☐ OK ☐ NOK ☐ N/A

IP Indemnification The supplier or partner defends, indemnifies and holds harmless the customer in the event of a third party claiming that the output generated by the services, products or activities of the supplier or partner violates their IP rights. Where restrictions and limitations apply to such IP indemnification, they have been defined and are acceptable.			✓			☐ OK ☐ NOK ☐ N/A
Guardrails The supplier or partner shall provide for guardrails and other features that will limit the AI input and output of its services, products and activities with regard to defined areas of problematic behavior or results, such as prohibited or unethical use, illegal content or infringement of third party rights. This may include the filtering or blocking of certain personal data or content, if data subjects or rights owners request so.	✓		✓		✓	☐ OK ☐ NOK ☐ N/A
Reliability The supplier or partner shall have its services, products and activities developed and implemented in such a manner that their AI output is of reasonable reliability, in particular in terms of correctness and completeness in view of its purpose. There are means to correct outputs for the future if the given reliability proves to be insufficient.				✓	✓	☐ OK ☐ NOK ☐ N/A
Abuse Monitoring It has been agreed whether only the supplier or partner, only the customer or both will or shall monitor the services, the use of the products or the activities for potential abusive use by their users.		✓			✓	☐ OK ☐ NOK ☐ N/A
Right to Use Output ★ The parties have agreed to which extent the customer (including its users) may use the output generated by or from the services, products or activities, including whether it may be used only for certain purposes or subject to other restrictions, who owns the output and whether additional payments may be required.			✓			☐ OK ☐ NOK ☐ N/A
Quality of AI Model Training The parties have defined the quality and other characteristics of the AI models to be used (including their training, testing and validation), and how these aspects shall be documented, measured and validated, as well as the remedies in case of non-compliance. If the services, products and activities include training or fine-tuning, such obligations shall apply accordingly.					✓	☐ OK ☐ NOK ☐ N/A
Acceptable Use Policy ★ The parties have agreed which restrictions will apply to the customer's (and its users') use of the services, products and activities, for instance that certain categories of content may not be generated or certain use cases are not permitted.			✓		✓	☐ OK ☐ NOK ☐ N/A
Amendment of Contract The parties have agreed how and under which conditions (i) the terms of the contract may be amended unilaterally, e.g., by new service terms on the part of the supplier or partner, and (ii) how new legal and regulatory requirements that reasonably require an amendment of the contract				✓	✓	☐ OK ☐ NOK ☐ N/A

are to be implemented (e.g., duty to negotiate an amendment).						
Liability/Indemnification The supplier or partner does neither unreasonably limit nor unreasonably exclude liability with regard to the known and unknown risks of AI. It shall provide for an adequate indemnification in the event that its violation of contract or law results in third party claims against the customer.					✓	☐ OK ☐ NOK ☐ N/A
Remedies in cases of breach of contract The parties have agreed on the remedies available to the customer and any other consequences if and when the supplier or partner fails to comply with the obligations agreed and warranties undertaken.					✓	☐ OK ☐ NOK ☐ N/A

Note: This checklist is provided for informational purposes only and is not legal advice. It is focused on European companies. If you see any errors or if you believe anything is missing, let us know at ai@vischer.com. The latest version can be found at https://vischerlnk.com/ai-provider-check. It is also available in German (https://vischerlnk.com/ki-provider-check). More information about AI is at https://vischer.com/ai, including a blog post (no. 15) providing further context to the above checklist.