Check out your GenAI project for risks.

Based on "GAIRA Light"

Do you plan to use an application based on generative AI in a company project? If so, then check out the following points.

Project: _____

Date: _____

1. Is your application likely to involve high risks for the company?

If you cannot confirm every of the following points, then your project likely involves high risks and you should do a comprehensive risk assessment (e.g., GAIRA Comprehensive). Otherwise proceed to step 2.

- We do not create or further train the AI model we use for our application (excluding "RAG") ☐
- We do not let our application take decisions on other people that they will find important ☐
- Our application will not interact with a large number of people concerning sensitive topics ☐
- We wouldn't consider legal steps even if a 3rd party used such an app against us/with our data ☐
- The application does not have a high potential to cause negative media headlines ("shitstorm") ☐
- The application does not qualify as a prohibited or high-risk system as per the EU AI Act ☐
- We will be using our AI application only for our purposes and not offer it to third parties ☐
- The application does not require a large investment, and it is not of strategic importance ☐

2. How are you dealing with the typical risks of generative AI?

If you cannot confirm every of the following points in view of the existing or planned measures to control the risks, then you should discuss the legal & reputational risks of your project internally.

- Our use of 3rd party confidential or protected data is in line with our contractual obligations ☐
- Our provider contracts are in line with data protection law and our other legal obligations ☐
- Our input/output will not be monitored by our provider(s) or we are fine with it ☐
- Our input/output will not be used by our provider(s) for their own purposes or we are fine with it ☐
- We have ensured that our AI solution will not leak confidential data or personal data to others ☐
- Our application neither systematically processes sensitive personal data nor does any profiling ☐
- We have a sufficient legal basis for processing personal data (where legally required) ☐
- We are using personal data only for one its original purposes (or one that had to be expected) ☐
- We limit the personal data collected/used to the minimum necessary for the purpose ☐
- We keep personal data in connection with the solution only for as long as needed ☐
- We are able to comply with data subject requests (e.g., access, correction, objection, deletion) ☐
- We have adequate data security and business continuity measures in place ☐
- We inform people about our use of AI where this is relevant for their interaction with us ☐
- The public and those affected by our use of AI will generally not find it unfair or objectionable ☐
- We have measures to avoid or deal with erroneous or other problematic output (e.g., bias) ☐
- Our application will be tested extensively prior to its use, including against adversarial use ☐
- Our use of AI does not cause unintended repercussions for others (e.g., damage, discrimination) ☐
- Our use of AI cannot be considered as being based on exploiting vulnerabilities of individuals ☐
- We have human oversight where our AI solution could take or influence key decisions ☐
- We will be using a widely recognized, quality AI model with a behavior we understand ☐
- Our use of AI will neither mislead nor deceive anyone ☐
- We have measures in place to detect any undesired behavior of our AI, to log it and to react to it ☐
- Our use of AI respects the dignity and individual autonomy of those affected by it ☐
- The users of our AI solution will be instructed, trained and monitored in its proper use ☐
- We do not foresee any other uncontrolled issue in connection with our use of AI ☐

If you are processing personal data, do not forget to also do a Data Protection Impact Assessment, amend your privacy notice and update your records of processing activities (ROPA), each where necessary. Also comply with your other company rules and procedures on AI, including ethical guidelines that may exist.

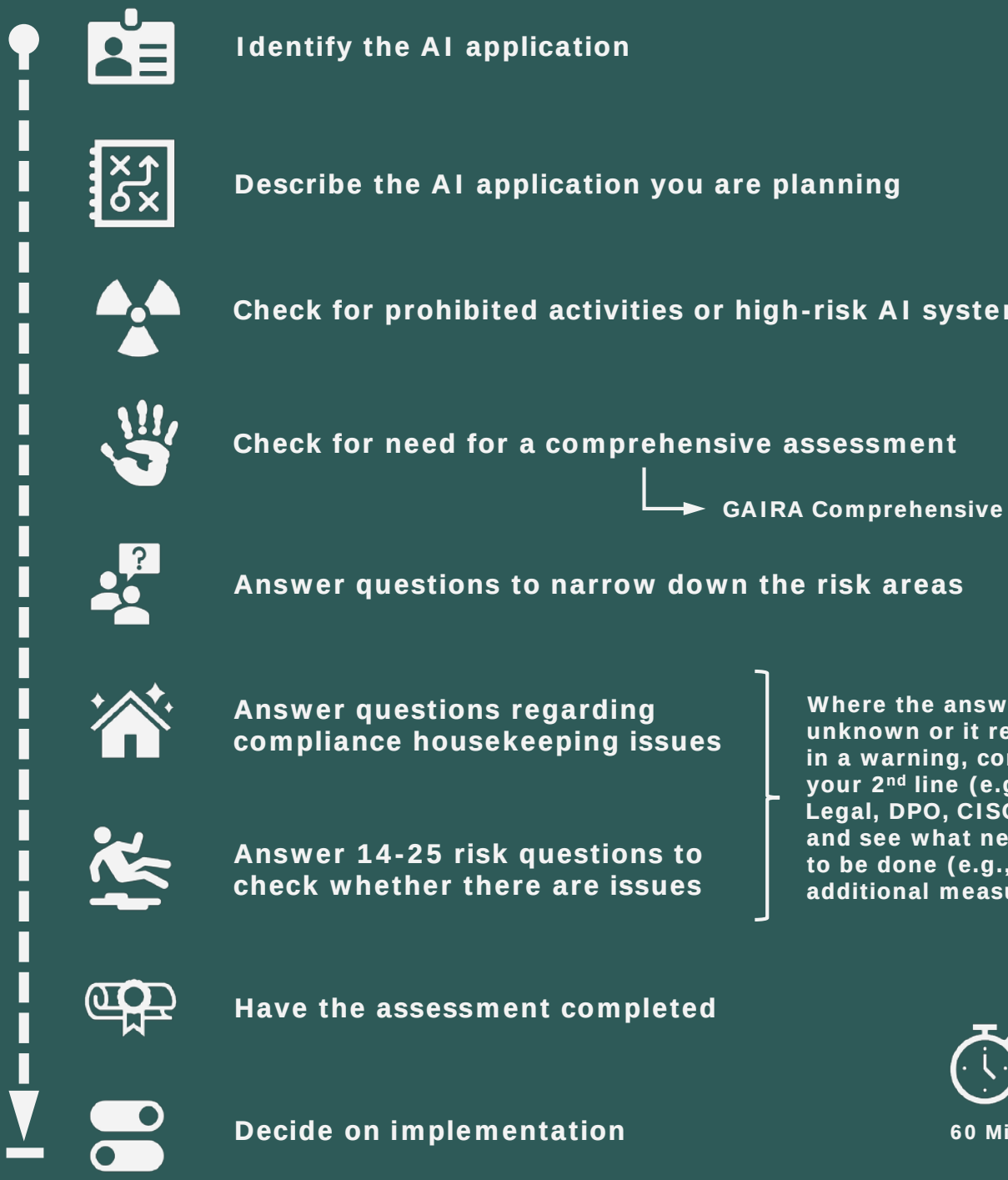
Do you want to properly document your above risk assessment? Get the GAIRA Excel for free at https://vischerlnk.com/gaira. It includes both a worksheet for the "Light" version with the points above and one for a comprehensive risk assessment and documentation.

Author: David Rosenthal (drosenthal@vischer.com) Updates: vischerlnk.com/update

VISCHER SWISS LAW AND TAX

Doing a risk assessment with GAIRA Light.

To assess your AI application project using GAIRA Light, you need to take the following nine steps. Expect 60 minutes to do so, unless it your project turns out to require a more comprehensive assessment (if high risk for the company are likely). You should be able to answer the questions on your own, possibly except for those related to the contracts of your provider(s). For those, ask your legal experts for advice.



Get the GAIRA excel for free at https://vischerlnk.com/gaira. It includes a worksheet for the "Light" version shown above and one for a comprehensive risk assessment. Note that the "Light" assessment does *not* include a "Data Protection Impact Assessment, which may be necessary, too. Discuss this with your DPO or other legal experts.

Author: David Rosenthal (drosenthal@vischer.com) Updates: vischerlnk.com/update

VISCHER
SWISS LAW AND TAX