VISCHER

# Generative AI.

## Handling risk management in practice & setting up an appropriate AI Governance Structure

Rolf Auf der Maur & David Rosenthal, VISCHER AG

AI House Davos

January 16, 2024

# Risks? There are many …

- Operational risks
- Legal & compliance risks
- Reputational risks

Understand, control and accept them

Business Continuity

Personality Rights

Copyright

Non-discrimination

Information Security

Consumer Protection

Other IP Rights

Competition Law

AI Ethics

AI Security

AI Regulations

Professional Secrecy

Provider contracts

General Regulations

Data Protection

Contractual Duties

# Some observations

- Many **existing rules** of law (e.g., data protection) **work well** also for GenAI; new regulations seem to target providers of AI
- Do not confuse legal requirements with **ethical principles**
- Expect a "legal" **demystification**; we will realize that with proper contracts and provider setups, feeding personal data and third-party content into GenAI systems is often less problematic than anticipated; the main concern is their output and its use
- Most GenAI projects are also **cloud projects**, which may result in additional requirements and issues for risk management
- A lack of **transparency** and **quality standards** concerning the models, their training, and AI offerings in general will continue to exist and make compliance and risk assessments difficult

# How to manage AI risks

1. Identify and discuss the applicable **compliance baseline**
2. Issue an appropriate **policy** for governing and using AI
3. Establish a proper **governance** (1st line, 2nd line, reporting)
4. Establish an **overview** of what is going on ("ROAIA")
5. Enable and **train** employees in the proper use of GenAI
6. Establish a process for a compliance and **risk assessment** of every AI service or other use of AI
7. Have the **2nd line assist** the 1st line in doing the assessment
8. Install **monitoring**, re-assessment and incident **reporting** processes and act upon findings and reports

# Doing AI risk assessments

- Many AI projects are **not very problematic**
  - E.g., using a chatbot for day-to-day tasks
- Is your AI project a **high-risk** for the company?
  - Training your own model
  - Taking important automated decisions
  - Interaction with many people on sensitive topcis
  - We would consider legal if this were about us
  - A high "shitstorm" factor
  - Prohibited activity or high-risk system as per EU AI Act
  - Offering AI applications to third parties
  - Large investment or project of strategic importance

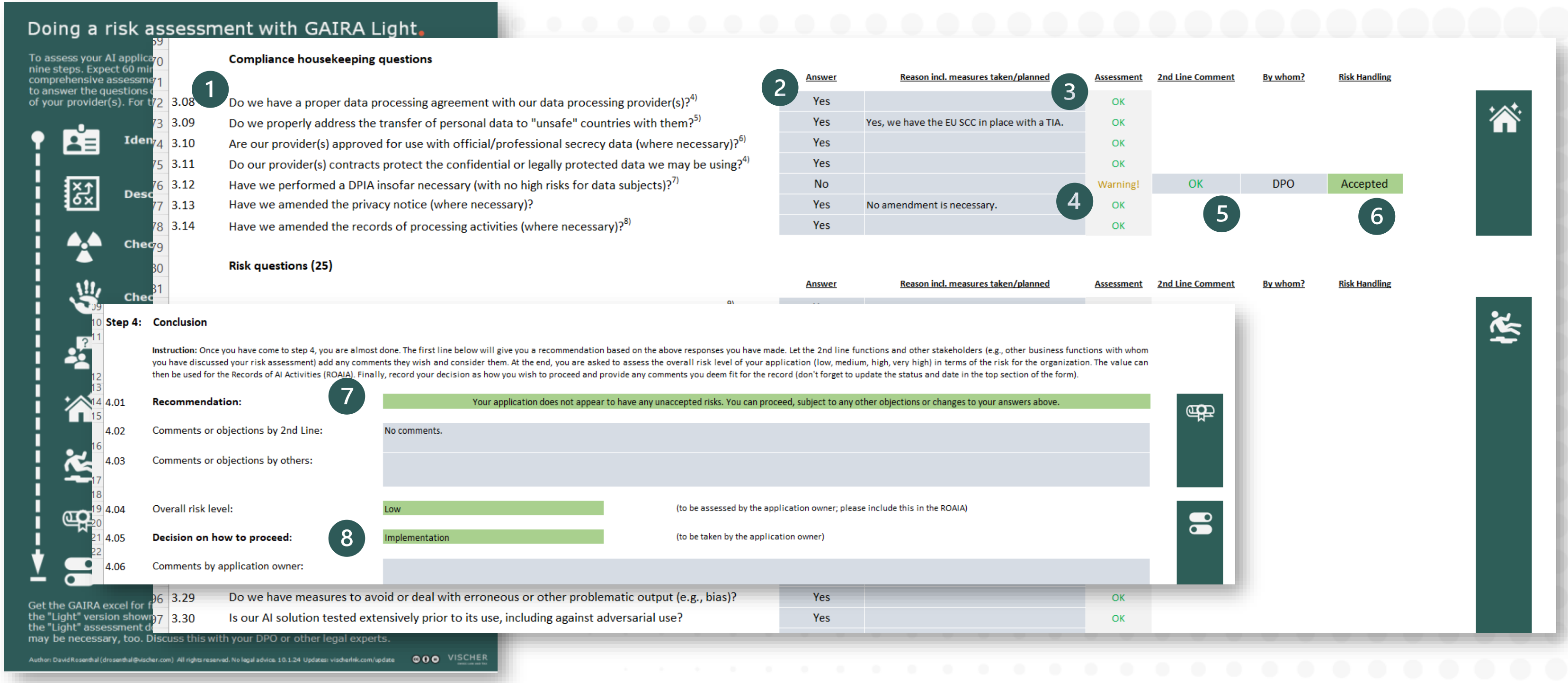
GAIRA Light

Get it at vischerlnk.com/gaira

GAIRA Comprehensive

If so, then do a comprehensive risk assessment

# GAIRA Light



Doing a risk assessment with GAIRA Light.

To assess your AI applica
nine steps. Expect 60 mi
comprehensive assessme
to answer the questions
of your provider(s). For t

**Compliance housekeeping questions**

| | | Answer | Reason incl. measures taken/planned | Assessment | 2nd Line Comment | By whom? | Risk Handling |
|---|---|---|---|---|---|---|---|
| 3.08 | Do we have a proper data processing agreement with our data processing provider(s)?[4] | Yes | | OK | | | |
| 3.09 | Do we properly address the transfer of personal data to "unsafe" countries with them?[5] | Yes | Yes, we have the EU SCC in place with a TIA. | OK | | | |
| 3.10 | Are our provider(s) approved for use with official/professional secrecy data (where necessary)?[6] | Yes | | OK | | | |
| 3.11 | Do our provider(s) contracts protect the confidential or legally protected data we may be using?[4] | Yes | | OK | | | |
| 3.12 | Have we performed a DPIA insofar necessary (with no high risks for data subjects)?[7] | No | | Warning! | OK | DPO | Accepted |
| 3.13 | Have we amended the privacy notice (where necessary)? | Yes | No amendment is necessary. | OK | | | |
| 3.14 | Have we amended the records of processing activities (where necessary)?[8] | Yes | | OK | | | |

**Risk questions (25)**

| | | Answer | Reason incl. measures taken/planned | Assessment | 2nd Line Comment | By whom? | Risk Handling |
|---|---|---|---|---|---|---|---|
| 3.29 | Do we have measures to avoid or deal with erroneous or other problematic output (e.g., bias)? | Yes | | OK | | | |
| 3.30 | Is our AI solution tested extensively prior to its use, including against adversarial use? | Yes | | OK | | | |

**Step 4: Conclusion**

**Instruction:** Once you have come to step 4, you are almost done. The first line below will give you a recommendation based on the above responses you have made. Let the 2nd line functions and other stakeholders (e.g., other business functions with whom you have discussed your risk assessment) add any comments they wish and consider them. At the end, you are asked to assess the overall risk level of your application (low, medium, high, very high) in terms of the risk for the organization. The value can then be used for the Records of AI Activities (ROAIA). Finally, record your decision as how you wish to proceed and provide any comments you deem fit for the record (don't forget to update the status and date in the top section of the form).

| | | | |
|---|---|---|---|
| 4.01 | **Recommendation:** | Your application does not appear to have any unaccepted risks. You can proceed, subject to any other objections or changes to your answers above. | |
| 4.02 | Comments or objections by 2nd Line: | No comments. | |
| 4.03 | Comments or objections by others: | | |
| 4.04 | Overall risk level: | Low | (to be assessed by the application owner; please include this in the ROAIA) |
| 4.05 | **Decision on how to proceed:** | Implementation | (to be taken by the application owner) |
| 4.06 | Comments by application owner: | | |

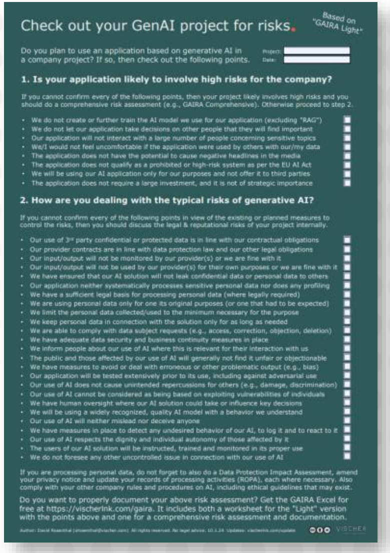
Get the GAIRA excel for f
the "Light" version show
the "Light" assessment d
may be necessary, too. Discuss this with your DPO or other legal experts.

Author: David Rosenthal (drosenthal@vischer.com) All rights reserved. No legal advice. 10.1.24 Updates: vischerlnk.com/update

VISCHER

# Ten questions to start with when using LLMs

- **Where** is the input ("prompts") sent to and processed?
- Is there a **data processing contract** with the provider?
- Is **data security** sufficiently ensured?
- Is the input used for **provider training** of the model?
- **What** input are employees allowed to make?
- Is the output ("completions") **monitored** by the provider?
- How do we deal with **inaccurate/unwanted output**?
- Must and can **"data leakage"** be avoided?
- Do we have to **point out** that we use AI and how?
- How do we handle **data subject requests** that we may get?



## 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/I would not feel uncomfortable if the application were used by others with our/my data □
- The application does not have the potential to cause negative headlines in the media □
- 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.

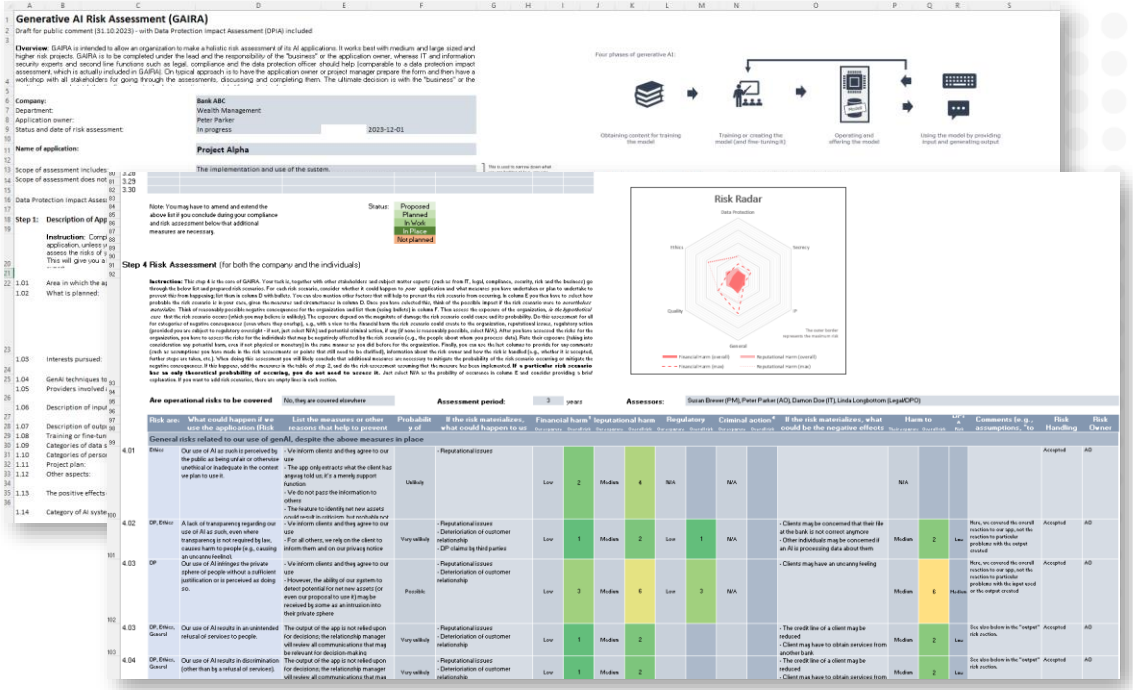
Do you want to properly document your above risk assessment? Get the GAIRA Excel for free at https://vischerlnk.com/gaira. It includes both a worksheet for the "Light" version with the points above and one for a comprehensive risk assessment and documentation.

Author: David Rosenthal (drosenthal@vischer.com) All rights reserved. No legal advice. 10.1.24 Updates: vischerlnk.com/update

VISCHER

vischerlnk.com/ai-riskcheck

# GAIRA Comprehensive / 1



**Generative AI Risk Assessment (GAIRA)**

Draft for public comment (31.10.2023) - with Data Protection Impact Assessment (DPIA) included

**Overview**: GAIRA is intended to allow an organization to make a holistic risk assessment of its AI applications. It works best with medium and large sized and higher risk projects. GAIRA is to be completed under the lead and the responsibility of the "business" or the application owner, whereas IT and information security experts and second line functions such as legal, compliance and the data protection officer should help (comparable to a data protection impact assessment, which is actually included in GAIRA). On typical approach is to have the application owner or project manager prepare the form and then have a workshop with all stakeholders for going through the assessments, discussing and completing them. The ultimate decision is with the "business" or the

| | |
|---|---|
| **Company:** | **Bank ABC** |
| Department: | Wealth Management |
| Application owner: | Peter Parker |
| Status and date of risk assessment: | In progress 2023-12-01 |
| **Name of application:** | **Project Alpha** |
| Scope of assessment includes: | The implementation and use of the system. |
| Scope of assessment does not | |
| Data Protection Impact Assess | |

**Step 1: Description of App**

**Instruction**: Compl application, unless y assess the risks of y This will give you a

| | |
|---|---|
| 1.01 | Area in which the a |
| 1.02 | What is planned: |
| 1.03 | Interests pursued: |
| 1.04 | GenAI techniques to |
| 1.05 | Providers involved i |
| 1.06 | Description of input |
| 1.07 | Description of outp |
| 1.08 | Training or fine-tuni |
| 1.09 | Categories of data s |
| 1.10 | Categories of perso |
| 1.11 | Project plan: |
| 1.12 | Other aspects: |
| 1.13 | The positive effects |
| 1.14 | Category of AI syste |

Four phases of generative AI:
Obtaining content for training the model
Training or creating the model (and fine-tuning it)
Operating and offering the model
Model
Using the model by providing input and generating output

3.28
3.29
3.30

Note: You may have to amend and extend the above list if you conclude during your compliance and risk assessment below that additional measures are necessary.

Status: Proposed / Planned / In Work / In Place / Not planned

**Step 4 Risk Assessment** (for both the company and the individuals)

**Instruction:** This step 4 is the core of GAIRA. Your task is, together with other stakeholders and subject matter experts (such as from IT, legal, compliance, security, risk and the business) go through the below list and prepared risk scenarios. For each risk scenario, consider whether it could happen to *your* application and what measures you have undertaken or plan to undertake to prevent this from happening; list them in column D with bullets. You can also mention other factors that will help to prevent the risk scenario from occurring. In column E you then have to select how probable the risk scenario is in your case, given the measures and circumstances in column D. Once you have selected this, think of the possible impact if the risk scenario were to *nevertheless materialize*. Think of reasonably possible negative consequences for the organization and list them (using bullets) in column F. Then assess the exposure of the organization, *in the hypothetical case* that the risk scenario occurs (which you may believe is unlikely). The exposure depend on the magnitude of damage the risk scenario could cause and its probability. Do this assessment for all for categories of negative consequences (even where they overlap), e.g., with a view to the financial harm the risk scenario could create to the organization, reputational issues, regulatory action (provided you are subject to regulatory oversight - if not, just select N/A) and potential criminal action, if any (if none is reasonably possible, select N/A). After you have assessed the risks for the organization, you have to assess the risks for the individuals that may be negatively affected by the risk scenario (e.g., the people about whom you process data). Rate their exposure (taking into consideration any potential harm, even if not physical or monetary) in the same manner as you did before for the organization. Finally, you can use the last columns to provide for any comments (such as assumptions you have made in the risk assessments or points that still need to be clarified), information about the risk owner and how the risk is handled (e.g., whether it is accepted, further steps are taken, etc.). When doing this assessment you will likely conclude that additional measures are necessary to mitigate the probability of the risk scenario occurring or mitigate the negative consequences. If this happens, add the measures in the table of step 2, and do the risk assessment assuming that the measure has been implemented. **If a particular risk scenario has an only theoretical probability of occuring, you do not need to assess it.** Just select N/A as the probility of occurance in column E and consider providing a brief explanation. If you want to add risk scenarios, there are empty lines in each section.

**Are operational risks to be covered** No, they are covered elsewhere

**Assessment period:** 3 years

**Assessors:** Susan Brewer (PM), Peter Parker (AO), Damon Doe (IT), Linda Longbottom (Legal/DPO)

| | Risk are: | What could happen if we use the application (Risk | List the measures or other reasons that help to prevent | Probability of | If the risk materializes, what could happen to us | Financial harm[1] | | Reputational harm | | Regulatory | | Criminal action[4] | | If the risk materializes, what could be the negative effects | Harm to | | DPIA Risk | Comments (e.g., assumptions, "to | Risk Handling | Risk Owner |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Our exposure | Overall risk | Our exposure | Overall risk | Our exposure | Overall risk | Our exposure | Overall risk | | Their exposure | Overall risk | | | | |
| | General risks related to our use of genAI, despite the above measures in place | | | | | | | | | | | | | | | | | | | |
| 4.01 | Ethics | Our use of AI as such is perceived by the public as being unfair or otherwise unethical or inadequate in the context we plan to use it. | - We inform clients and they agree to our use<br>- The app only extracts what the client has anyway told us; it's a merely support function<br>- We do not pass the information to others<br>- The feature to identify net new assets could result in criticism, but probably not | Unlikely | - Reputational issues | Low | 2 | Medium | 4 | N/A | | N/A | | | N/A | | | | Accepted | AO |
| 4.02 | DP, Ethics | A lack of transparency regarding our use of AI as such, even where transparency is not required by law, causes harm to people (e.g., causing an uncanny feeling). | - We inform clients and they agree to our use<br>- For all others, we rely on the client to inform them and on our privacy notice | Very unlikely | - Reputational issues<br>- Deterioriation of customer relationship<br>- DP claims by third parties | Low | 1 | Medium | 2 | Low | 1 | N/A | | - Clients may be concerned that their file at the bank is not correct anymore<br>- Other individuals may be concerned if an AI is processing data about them | Medium | 2 | Low | Here, we covered the overall reaction to our app, not the reaction to particular problems with the output created | Accepted | AO |
| 4.03 | DP | Our use of AI infringes the private sphere of people without a sufficient justification or is perceived as doing so. | - We inform clients and they agree to our use<br>- However, the ability of our system to detect potential for net new assets (or even our proposal to use it) may be received by some as an intrusion into their private sphere | Possible | - Reputational issues<br>- Deterioriation of customer relationship | Low | 3 | Medium | 6 | Low | 3 | N/A | | - Clients may have an uncanny feeling | Medium | 6 | Medium | Here, we covered the overall reaction to our app, not the reaction to particular problems with the input used or the output created | Accepted | AO |
| 4.03 | DP, Ethics, General | Our use of AI results in an unintended refusal of services to people. | The output of the app is not relied upon for decisions; the relationship manager will review all communications that may be relevant for decision-making | Very unlikely | - Reputational issues<br>- Deterioriation of customer relationship | Low | 1 | Medium | 2 | | | | | - The credit line of a client may be reduced<br>- Client may have to obtain services from another bank | Medium | 2 | Low | See also below in the "output" risk section. | Accepted | AO |
| 4.04 | DP, Ethics, General | Our use of AI results in discrimination (other than by a refusal of services). | The output of the app is not relied upon for decisions; the relationship manager will review all communications that may | Very unlikely | - Reputational issues<br>- Deterioriation of customer relationship | Low | 1 | Medium | 2 | | | | | - The credit line of a client may be reduced<br>- Client may have to obtain services from | Medium | 2 | Low | See also below in the "output" risk section. | Accepted | AO |

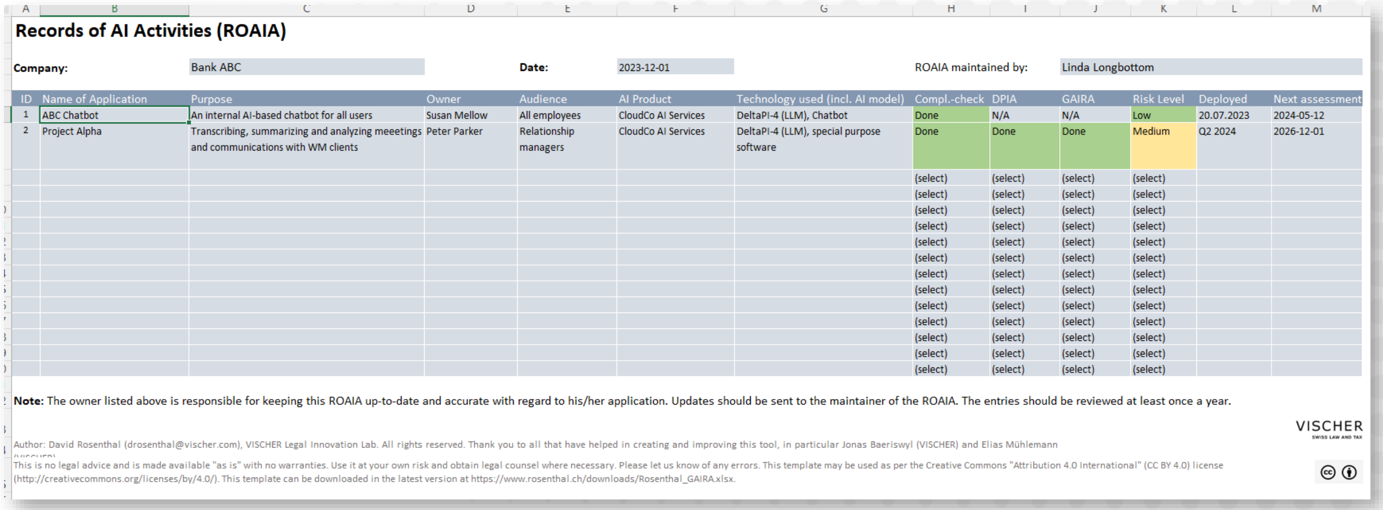
- Full AI risk assessment including a data protection impact assessment (DPIA)
- Requires a list of technical and organizational measures
- Requires more time (several hours for the business to complete)
- Covers also reputational risks

Available for free at vischerlnk.com/gaira

# GAIRA Comprehensive / 2

- Use the **same** proven **approach** as for doing a **DPIA**
  - Have the application owner describe the application
  - Have the application owner list all measures intended to prevent "problems" and to comply with law and internal policies
  - Go through the list of risk scenarios, and have the application owner and others assess the relevant risks; typically, additional measures will pop-up – add them to the list of measures
  - Ensure that someone is responsible for each measure
- **Top five DP risks** are usually accuracy, secrecy, data leakage, provider contracts and data subject rights
  - Ethics and transparency are usually not (yet) an issue
- Don't forget: The application **owner**/business has to **decide**

# Creating the "ROAIA"



**Records of AI Activities (ROAIA)**

**Company:** Bank ABC

**Date:** 2023-12-01

ROAIA maintained by: Linda Longbottom

| ID | Name of Application | Purpose | Owner | Audience | AI Product | Technology used (incl. AI model) | Compl.-check | DPIA | GAIRA | Risk Level | Deployed | Next assessment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ABC Chatbot | An internal AI-based chatbot for all users | Susan Mellow | All employees | CloudCo AI Services | DeltaPI-4 (LLM), Chatbot | Done | N/A | N/A | Low | 20.07.2023 | 2024-05-12 |
| 2 | Project Alpha | Transcribing, summarizing and analyzing meeetings and communications with WM clients | Peter Parker | Relationship managers | CloudCo AI Services | DeltaPI-4 (LLM), special purpose software | Done | Done | Done | Medium | Q2 2024 | 2026-12-01 |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |
| | | | | | | | (select) | (select) | (select) | (select) | | |

**Note:** The owner listed above is responsible for keeping this ROAIA up-to-date and accurate with regard to his/her application. Updates should be sent to the maintainer of the ROAIA. The entries should be reviewed at least once a year.

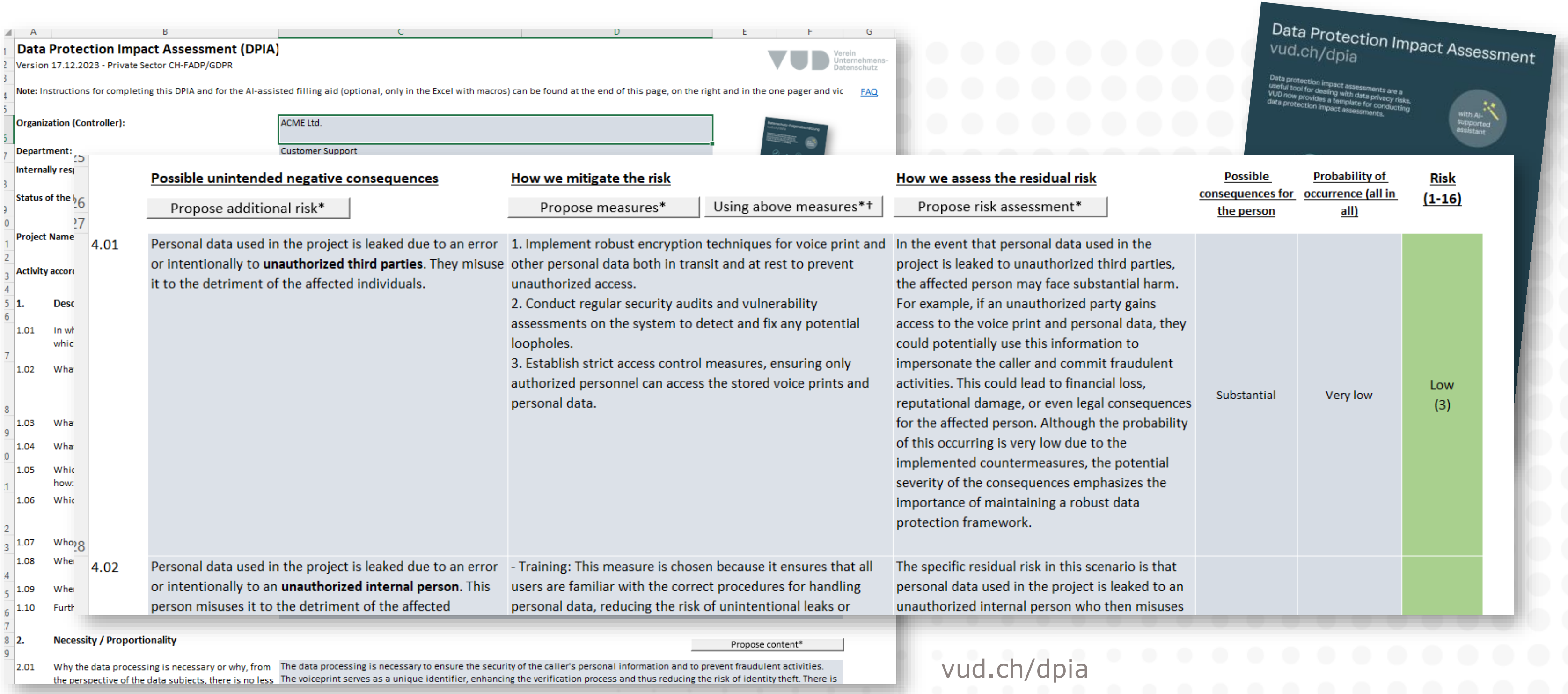
VISCHER
SWISS LAW AND TAX

Author: David Rosenthal (drosenthal@vischer.com), VISCHER Legal Innovation Lab. All rights reserved. Thank you to all that have helped in creating and improving this tool, in particular Jonas Baeriswyl (VISCHER) and Elias Mühlemann (VISCHER)

Download it at vischerlnk.com/gaira

What works well for data protection (the "Records of Processing Activities" or ROPA), also works well for AI applications ("Records of AI Activities")

# AI helping out on DP risk assessments



**Data Protection Impact Assessment (DPIA)**
Version 17.12.2023 - Private Sector CH-FADP/GDPR

**Note:** Instructions for completing this DPIA and for the AI-assisted filling aid (optional, only in the Excel with macros) can be found at the end of this page, on the right and in the one pager and vic FAQ

| | |
|---|---|
| **Organization (Controller):** | ACME Ltd. |
| **Department:** | Customer Support |
| **Internally res** | |
| **Status of the** | |
| **Project Name** | |
| **Activity accor** | |
| **1.** **Desc** | |
| 1.01 In wh whic | |
| 1.02 Wha | |
| 1.03 Wha | |
| 1.04 Wha | |
| 1.05 Whic how: | |
| 1.06 Whic | |
| 1.07 Who | |
| 1.08 Whe | |
| 1.09 Whe | |
| 1.10 Furth | |

| | **Possible unintended negative consequences** | **How we mitigate the risk** | | **How we assess the residual risk** | **Possible consequences for the person** | **Probability of occurrence (all in all)** | **Risk (1-16)** |
|---|---|---|---|---|---|---|---|
| | Propose additional risk* | Propose measures* | Using above measures*† | Propose risk assessment* | | | |
| 4.01 | Personal data used in the project is leaked due to an error or intentionally to **unauthorized third parties**. They misuse it to the detriment of the affected individuals. | 1. Implement robust encryption techniques for voice print and other personal data both in transit and at rest to prevent unauthorized access.<br>2. Conduct regular security audits and vulnerability assessments on the system to detect and fix any potential loopholes.<br>3. Establish strict access control measures, ensuring only authorized personnel can access the stored voice prints and personal data. | | In the event that personal data used in the project is leaked to unauthorized third parties, the affected person may face substantial harm. For example, if an unauthorized party gains access to the voice print and personal data, they could potentially use this information to impersonate the caller and commit fraudulent activities. This could lead to financial loss, reputational damage, or even legal consequences for the affected person. Although the probability of this occurring is very low due to the implemented countermeasures, the potential severity of the consequences emphasizes the importance of maintaining a robust data protection framework. | Substantial | Very low | Low<br>(3) |
| 4.02 | Personal data used in the project is leaked due to an error or intentionally to an **unauthorized internal person**. This person misuses it to the detriment of the affected | - Training: This measure is chosen because it ensures that all users are familiar with the correct procedures for handling personal data, reducing the risk of unintentional leaks or | | The specific residual risk in this scenario is that personal data used in the project is leaked to an unauthorized internal person who then misuses | | | |

**2.** **Necessity / Proportionality** Propose content*

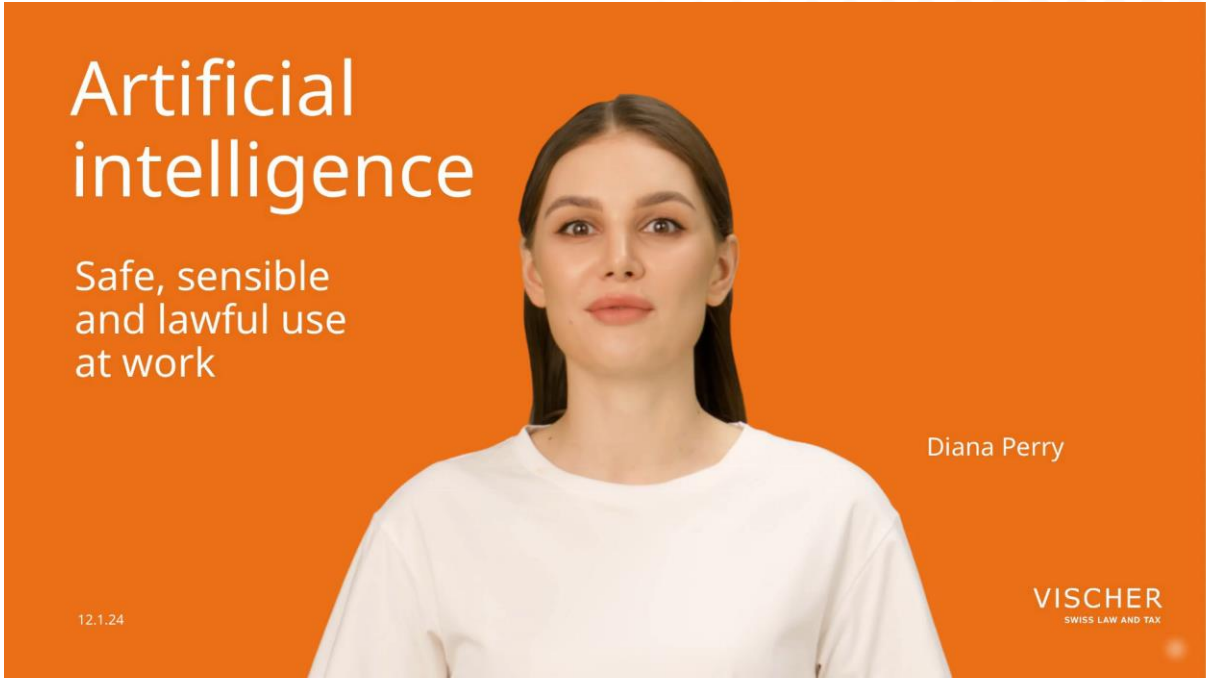
2.01 Why the data processing is necessary or why, from the perspective of the data subjects, there is no less — The data processing is necessary to ensure the security of the caller's personal information and to prevent fraudulent activities. The voiceprint serves as a unique identifier, enhancing the verification process and thus reducing the risk of identity theft. There is

Data Protection Impact Assessment
vud.ch/dpia

Data protection impact assessments are a useful tool for dealing with data privacy risks. VUD now provides a template for conducting data protection impact assessments.

vud.ch/dpia

# An AI that warns and charms about her kind



Artificial intelligence

Safe, sensible and lawful use at work

Diana Perry

12.1.24

VISCHER
SWISS LAW AND TAX

Feel free to share the video in your office with anyone you think should learn the three key points Diana presents

vischerlnk.com/ai-intro

http://www.youtube.com/@VISCHERLegalInnovationLab

# AI Governance in Practice

- Does your organization need an AI Compliance Officer?
- Which department is the most appropriate for AI Compliance?
- What are the rights and obligations of the AI Compliance Officer?
- Should AI Principles be adopted and implemented (law and ethics)?
- Does every AI Application have a business owner (accountability)?
- Which risk assessment methodology should be applied?
- Should a standard be adopted (voluntarily)?
- ISO/IEC 42001Standard on AI management system (AIMS), adapted on 18 December 2023
- Artificial Intelligence Risk Management Framework (AI RMF 1.0) by the U.S. National Institute for Standards and Technology
- Sanctions for non compliance?

AI Governance
Roles
Responsibilities
Standards
Sanctions

# TBD: Corporate AI Principles

- 11 Principles for the responsible use of AI:
  - We ensure accountability
  - We provide the necessary transparency
  - We remain fair and do no harm
  - We ensure reliability
  - We ensure information security
  - We pay attention to proportionality and self-determination
  - We respect others' and our own intellectual property
  - We protect the rights of those affected
  - We ensure explainability and human oversight
  - We understand and control the risks
  - We prevent misuse of our AI applications

AI Principles
Legal
Ethics
Corporate
Culture

VISCHER

AIgen

# Thank you for your attention!

Questions: drosenthal@vischer.com, ram@vischer.com

**Zürich**
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

**Basel**
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

**Genf**
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com

Visit vischer.com/ai and the
VISCHER Legal Innovation Lab
vischer.com/en/lil