Nordcloud
an IBM Company

Embedding legal, security and ethical topics in your solution.

How the ‘boring’ stuff makes your solution more sellable.

Cécile Trachsel, Project Manager / Henning Büsch, Senior GRC Advisor

Clients talking compliance

Agenda.

1. Introduction: why are they acting that way?
2. AI Journey.
3. What you can do.

Nordcloud
an IBM Company

Clients talking compliance

The environment you are selling into.

Sales process

An enterprise customer is interested in your solution. After the initial talks, things seem to slow down.

Regulatory development

New requirements, such as NIS-2, DORA, GDPR, revDSG, EU AI Act requiring companies to perform due diligence

Impact to companies

After the initial sales process, companies require detailed information about the security, architecture, and legal aspects

Impact to sales process

You may encounter longer processes, questionnaires and more questions

Preparation

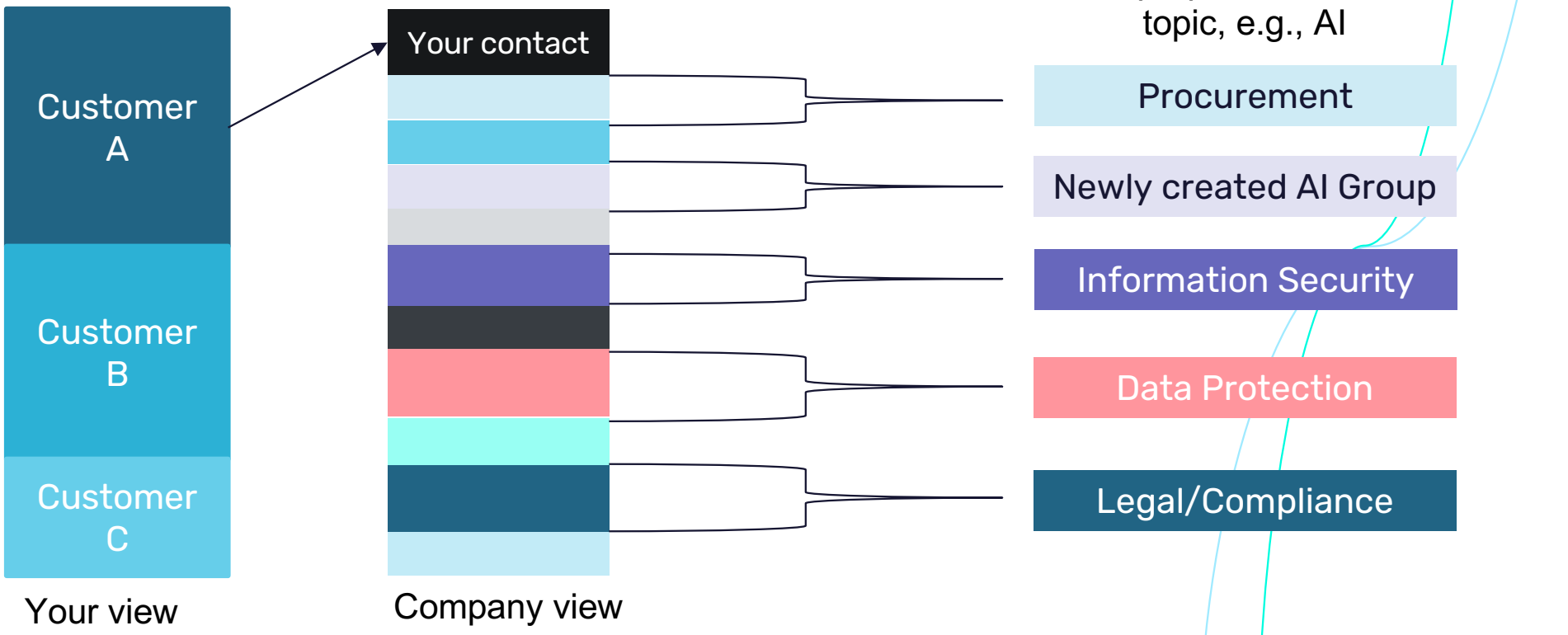
However, the information required is likely to be same for many customers so you can prepare

Requirements: e.g. (cyber) risk management, data protection, incident response, supply chain security, security measures, notification of breach, business continuity, governance

Nordcloud
an IBM Company

Clients talking compliance

Your landscape.



Nordcloud
an IBM Company

Clients talking compliance

AI enters the field.

Aspects

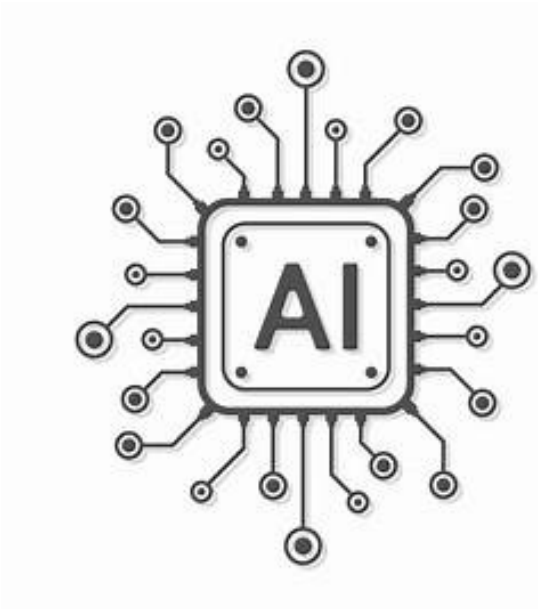
New aspects and yet many principles remain the same from cloud topics

Communalities

Shared Responsibility Model
Information Security aspects
General approach

Differences

Frameworks, standards, interpretations are still evolving
Lack of maturity of customers including data governance



New ISO standards published and in preparation

Nordcloud
an IBM Company

AI Act

What is the EU AI Act?

The EU AI Act is a regulatory framework set by the European Commission to ensure AI systems in the EU market are safe, ethical, and aligned with fundamental rights.

Scope: Applies to AI providers, deployers, and users within the EU and companies outside the EU if their AI systems affect EU citizens.

Purpose:

- Ensure AI technologies are used safely and responsibly.
- Safeguard transparency, accountability and responsibility during AI development.
- Mitigate AI risks, such as bias, discrimination, security vulnerabilities.
- Promote innovation by creating clear compliance guidelines.

Timeline:

- Apr21: EU Commission proposes the AI Act.
- Aug24: AI Act legally binding, although requirements gradually rolled out
- Feb25: Forbidden AI systems are banned, AI literacy required.
- Aug25: EU governance, General Purpose AI rules, penalties for prohibited AI
- Aug26: AI Act applies, including requirements and penalties for high-risk AI

Clients talking compliance

Risk based classification system

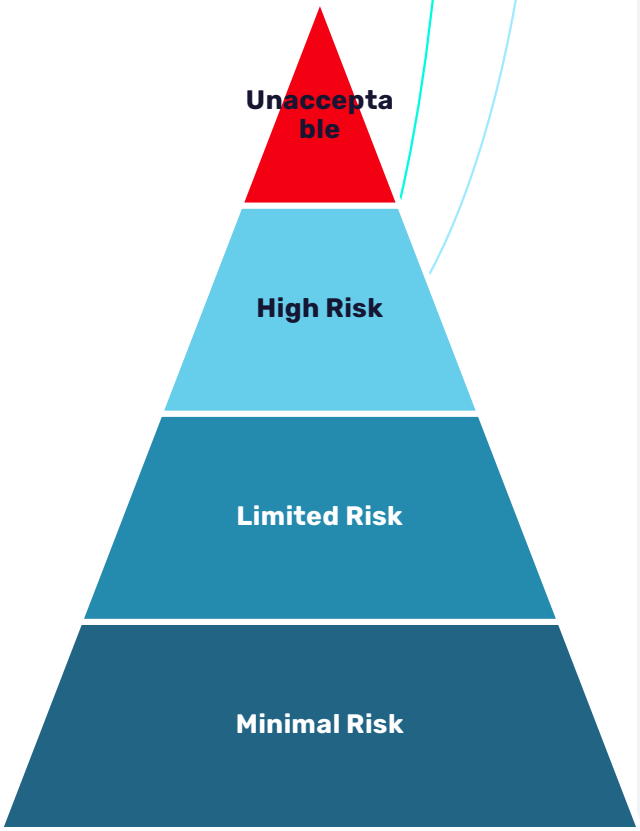
1. **Unacceptable Risk.** Forbidden AI practices, restriction in personal freedom. For example: social scoring, manipulation, emotion recognition in workplaces, biometric categorization (Feb25)

2. **High Risk.** Heavy regulated AI systems, with big impact on personal life. For example: automatic CV selection, marking exams, determining loans, reliability of evidence (Aug26)

3. **Limited Risk.** Transparency obligations for AI systems with limited impact. For example: chatbots, systems that generate texts and images,

4. **Minimal Risk.** Not regulated AI systems. For Example: spam filters, AI in video games or product recommendations.

Note that beyond requirements of the AI Act, other laws & regulations also apply, like **GDPR** for processing privacy data or the **Digital Operational Resilience Act (DORA)** for financial institutions.



Nordcloud
an IBM Company

Clients talking compliance

And .. there will be questionnaires.

Clients talking compliance

AI Risk layers

Model risks

Risks related to the training, development and performance of the AI system

Data risks

Risks related to the collection, processing, storage, management and usage of data

Infrastructure risks

Risks related to the acquisition, implementation and operation of an AI system (incl. software and technology environment)

Operational risks

Risks related to the intentional or unintentional misuse, manipulation of, or attacks against an AI system

Process and application integration risks
Risks resulting from integrating AI/ML models into applications, workflows and processes

Legal and compliance risks
Noncompliance with applicable law, rules and industry-specific regulations (e.g. privacy, sector, function)

Nordcloud
an IBM Company

Clients talking compliance

Focus areas depending on area.

Governance

Provider

- Quality Management System
- Risk Management System
- RACI model
- Data Sourcing
- Model training
- Testing and verification
- Design choices
- Model access and dissemination

Model

LLM

Model characteristics:

- Information Security
- Performance
- Truthfulness
- Robustness
- Model limit
- User instructions

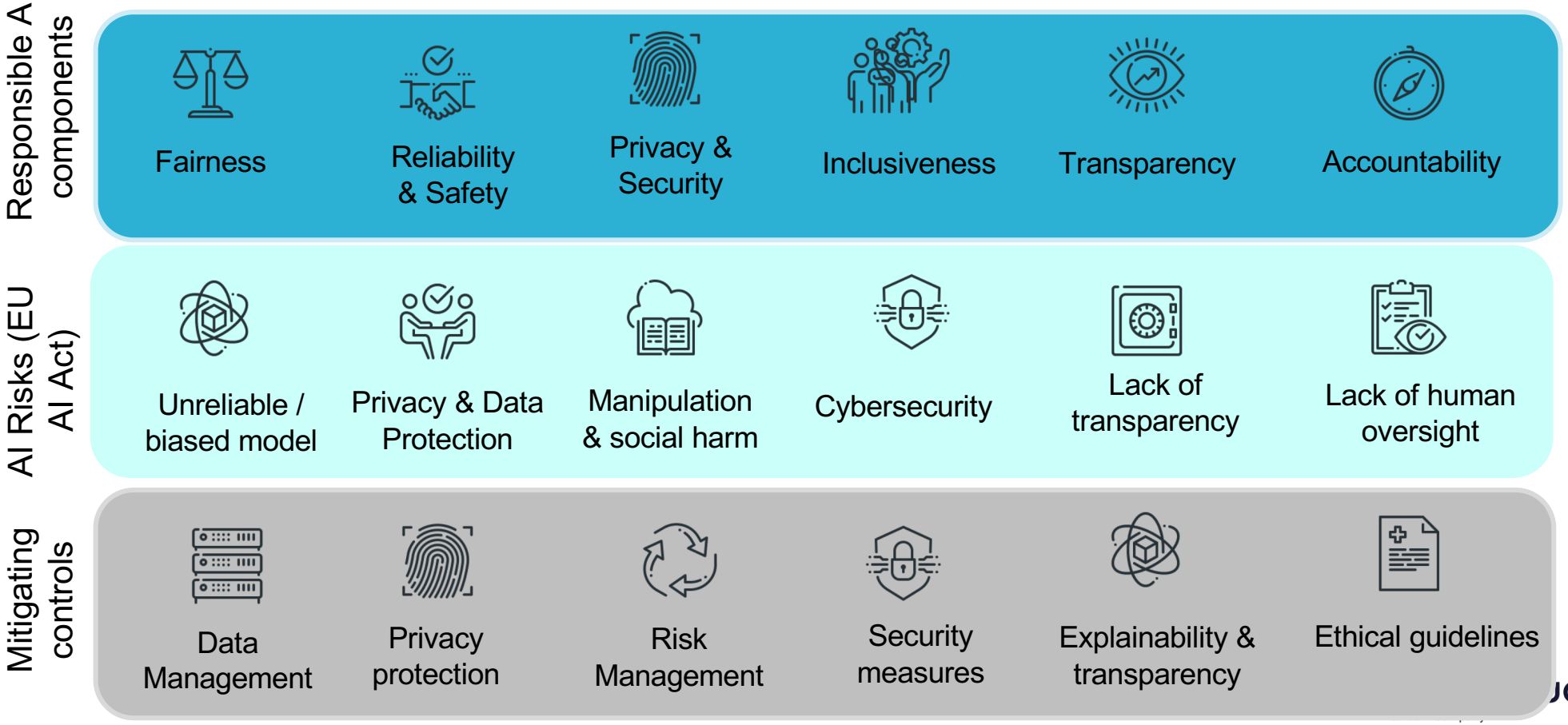
Application

Application-specific

- Use case design
- Functionality
- Sector specific requirements
- Impact
- Bias & discrimination
- Complaints management

Nordcloud
an IBM Company

Principles – Risks – Mitigating controls



Clients talking compliance

Topics to consider.

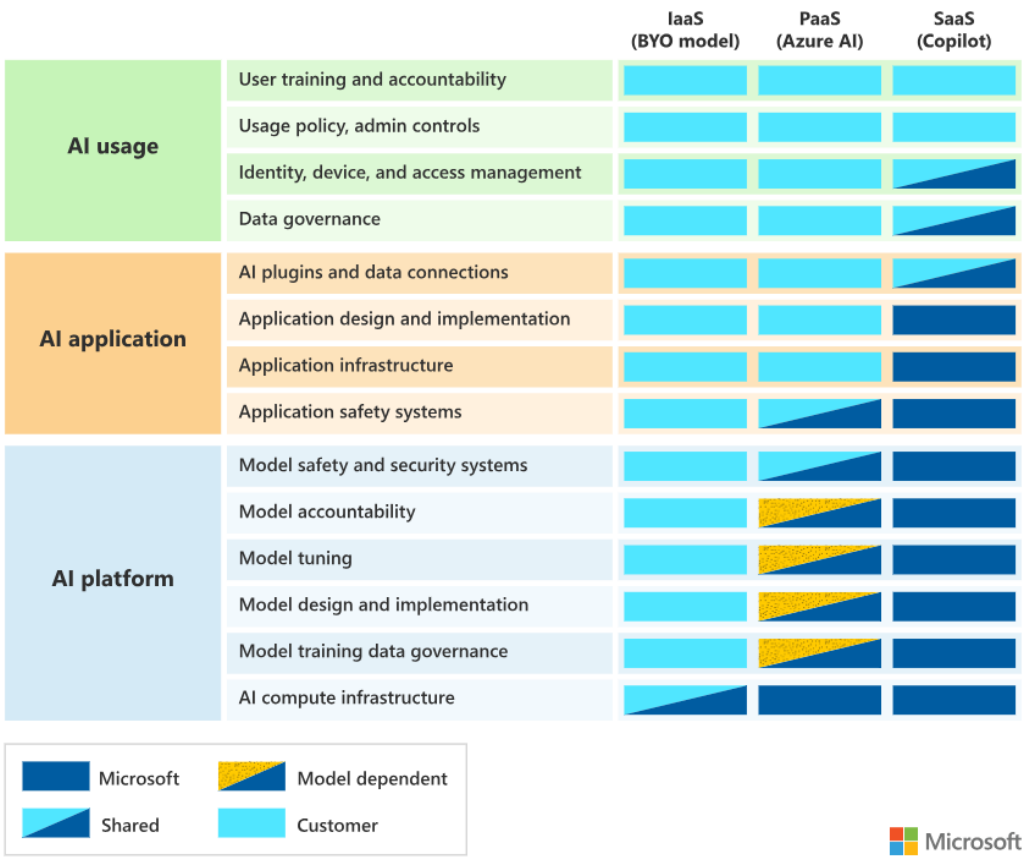
Following is a list of typical questions we hear from AI customers or have been asked by AI startups. Pro-active step from your side:

- Understand the requirements of your customer.
- Understand how your solution is classified in the EU AI Act. If you provide a solution considered as high-risk, understand the implications also for your customers.
- Understand their approval processes, e.g. is there a formal acceptance process for the company-wide usage of an AI tool.
- Build one/two/three pagers for your customer stakeholders.
- This will save you time instead of answering these questions again and again.
- And it will position you as a solution provider who has already considered these topics in the design of the solution rather than these topics being an after though.

Nordcloud
an IBM Company

Clients talking compliance

Understanding the shared responsibility model.



Microsoft

Question :

What is within my area of responsibility? How is the contractual relationship?

How should I consider copyright-relevant content? Is this something the customer has to consider or is it my problem? (Shared responsibility *Customer Copyright Commitment Required Mitigations – next slides*)

Who has the contractual obligation that a solution is build in accordance with a certain law, e.g. data protection? *(Customer – w/ applicable laws)*

How can I check that my contracts and data protection addendums are in line with customer expectations?

Nordcloud
an IBM Company

How should I consider copyright-relevant content? Is this something the customer has to consider or is it my problem?

In my view the developer of a system has certain responsibilities. However, I see two different situations: If you create your own LLM, you are responsible to make sure to not violate any copyright (see also case of American authors against ChatGPT). In the other case, if you provide a solution, you need consider technical measurements to mitigate copyright violations (e.g. content filter (Azure OpenAI in Azure AI Foundry Models content filtering - Azure OpenAI | Microsoft Learn)). You may also include contractual commitments of the vendors of the AI system to defer your risk (e.g. Customer Copyright Commitment Required Mitigations | Microsoft Learn). Of course you can also try to mitigate this risk by adding specific contractual commitments between you and your customer.
Copilot shared an blog post of Visher about this topic in the context of Swiss law: Part 10: Copyright and AI: Responsibility of providers and users - VISCHER

•Who has the contractual obligation that a solution is build in accordance with a certain law, e.g. data protection?

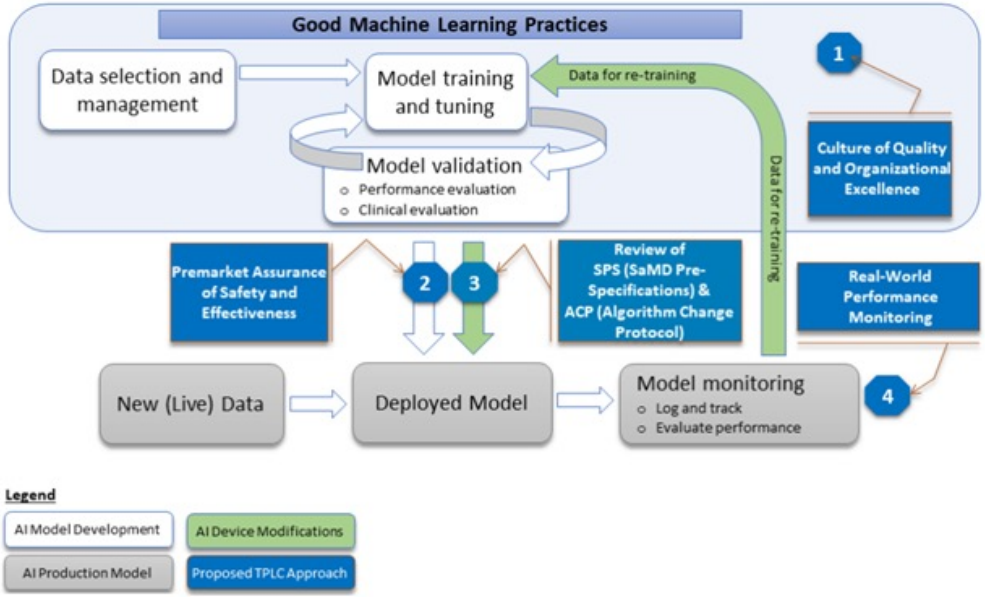
Finally, it's always the customer that decides if they implement a solution or not. A customer will always focus on the risk they take according to the specific regulations they have to apply to. The customer will do a risk assessment, evaluating mitigation steps and then decide if they are willing to take the residual risks or not.
The provider of a solution may not know all the details of the regulations his customer has to apply to (and it's the final decision of the customer). But it would be good if the provider has an understanding about the main regulatory requirements of his focus customers. A provider of a solution should always understand the dimensions of protection data at rest, data in transit and data in use and how his solution would support customers here. You can also use various options to address a risk.

How can I check that my contracts and data protection addendums are in line with customer expectations?

I would start with the solution in mind first and trying to understand the requirements for data at rest, data in transit and data in use from a high level. If you think you have the right answers, I would propose my solution to a Data Protection Officer (DPO) of my customer and ask him for his feedback. Based on the feedback, you may adapt your solution.
If you know you solution would work, you should already have a good understanding about what is needed in your contracts. You may be able to use other contracts as a starting point. However, it's always recommended to involve your lawyer (internal or external) to help you with the contract. You get the final proof if the contract matches all the requirements of your customer when you try to close the deal...

Clients talking compliance

Creating output.



Example from FDA Good Machine Learning Practice re reference data, oversight, validation and testing methods for algorithms, models and claims

Question :

How do you keep sure that we are seeing the right output? How to I ensure transparency over how output is generated and compliant with responsible AI practices? (see next slides)

What are best ways to sanitize data? (input output – masking, filtering, content safety – new service Content Safety,… OWASP top 10, DLP egress..)

My customer asks for adherence to storage limitation principles, e.g. data is deleted after three months after extraction? *(depending on storage technology, example storage blob and* *Configure a lifecycle management policy - Azure Blob Storage | Microsoft Learn*)

Nordcloud
an IBM Company

Automated evaluation in Azure AI Foundry

Text

Quality

AI-assisted metrics

Groundedness

Coherence

Fluency

Relevance

Retrieval score

Similarity

NLP metrics

F1 score, BLEU, ROUGE, GLEU, METEOR

Text + Image

Risk & safety

AI-assisted metrics

Hate and unfairness

Sexual

Violence

Self-harm

Protected materials

Text

Risk & safety

AI-assisted metrics

Direct attack jailbreak

Indirect attack jailbreak

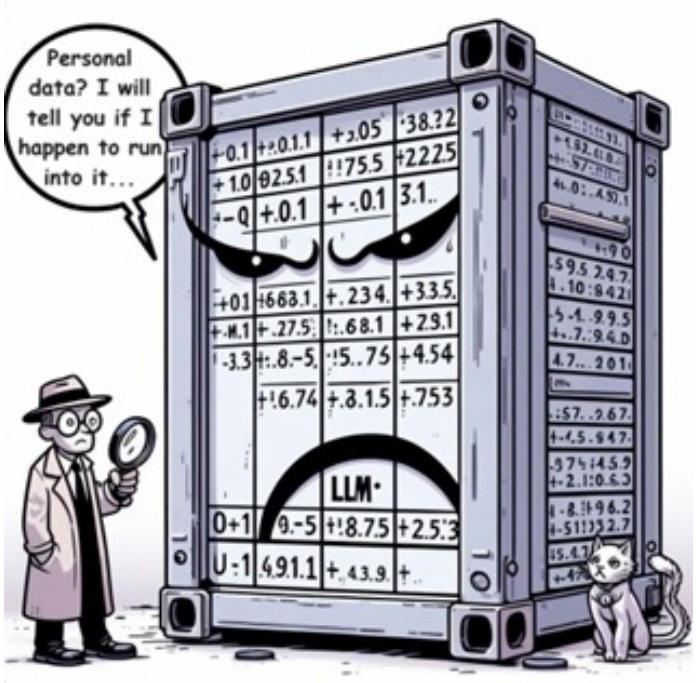
Text

Custom

Customize pre-built metrics or build your own metrics or synthetic data simulator with Azure AI Evaluation SDK

Clients talking compliance

Data protection considerations.



Questions:

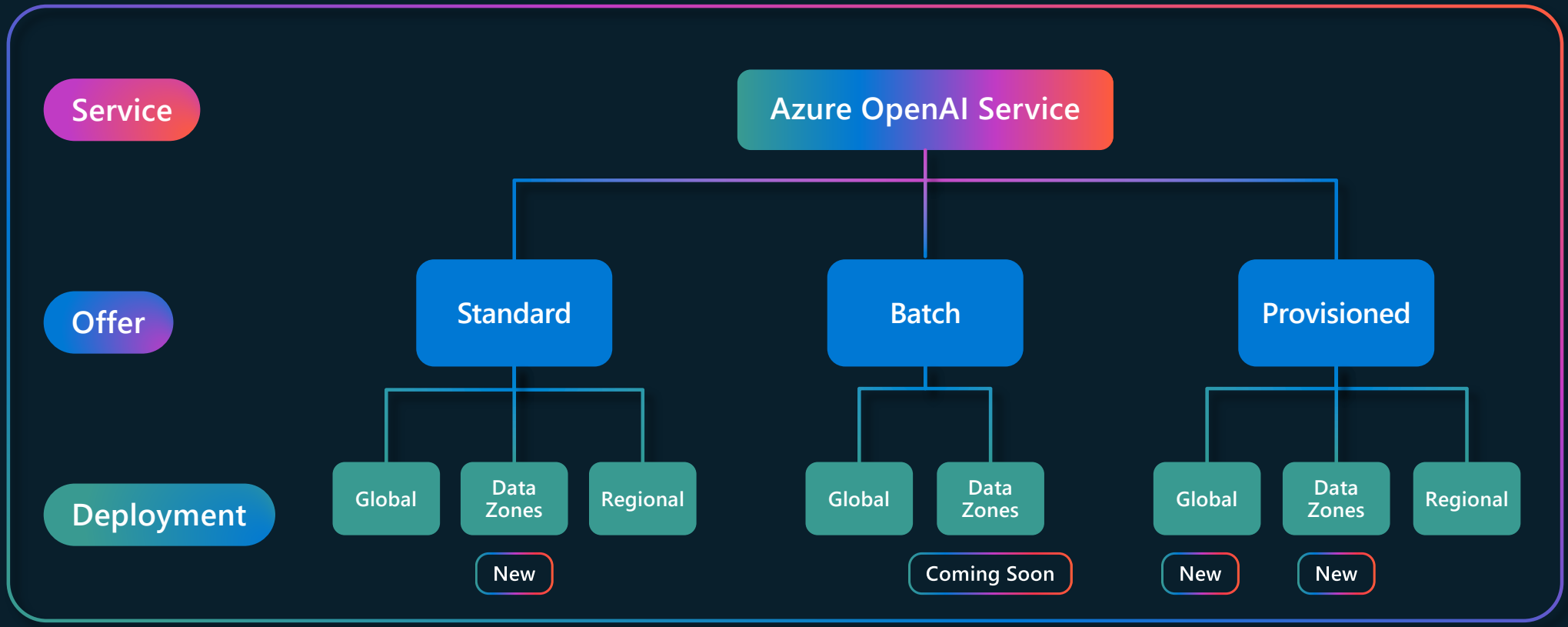
How is the usage of Embedded Models and AzureOpenAI API handled from a data protection perspective? How can I make sure that customer data is not used to train, retrain or improve the LLM model I use? (part of our commitment)

How can it be ensured when using AzureOpenAI that the data remains within a specified Azure region and is not transmitted to Open AI? In general , how I can ensure that the data does not leave Switzerland (or any other location) ? (*next slides*)

Nordcloud
an IBM Company

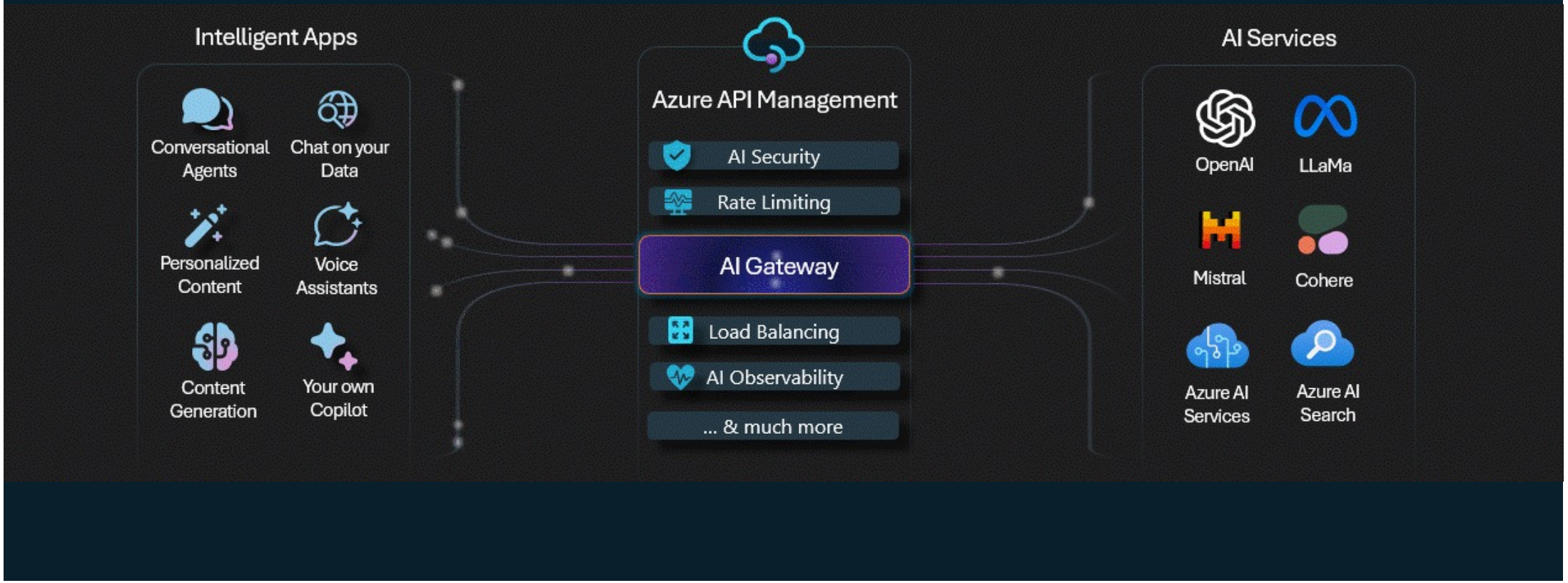
Azure OpenAI Service Offerings

...ensuring everyone understands which regions data can travel to or can be processed in

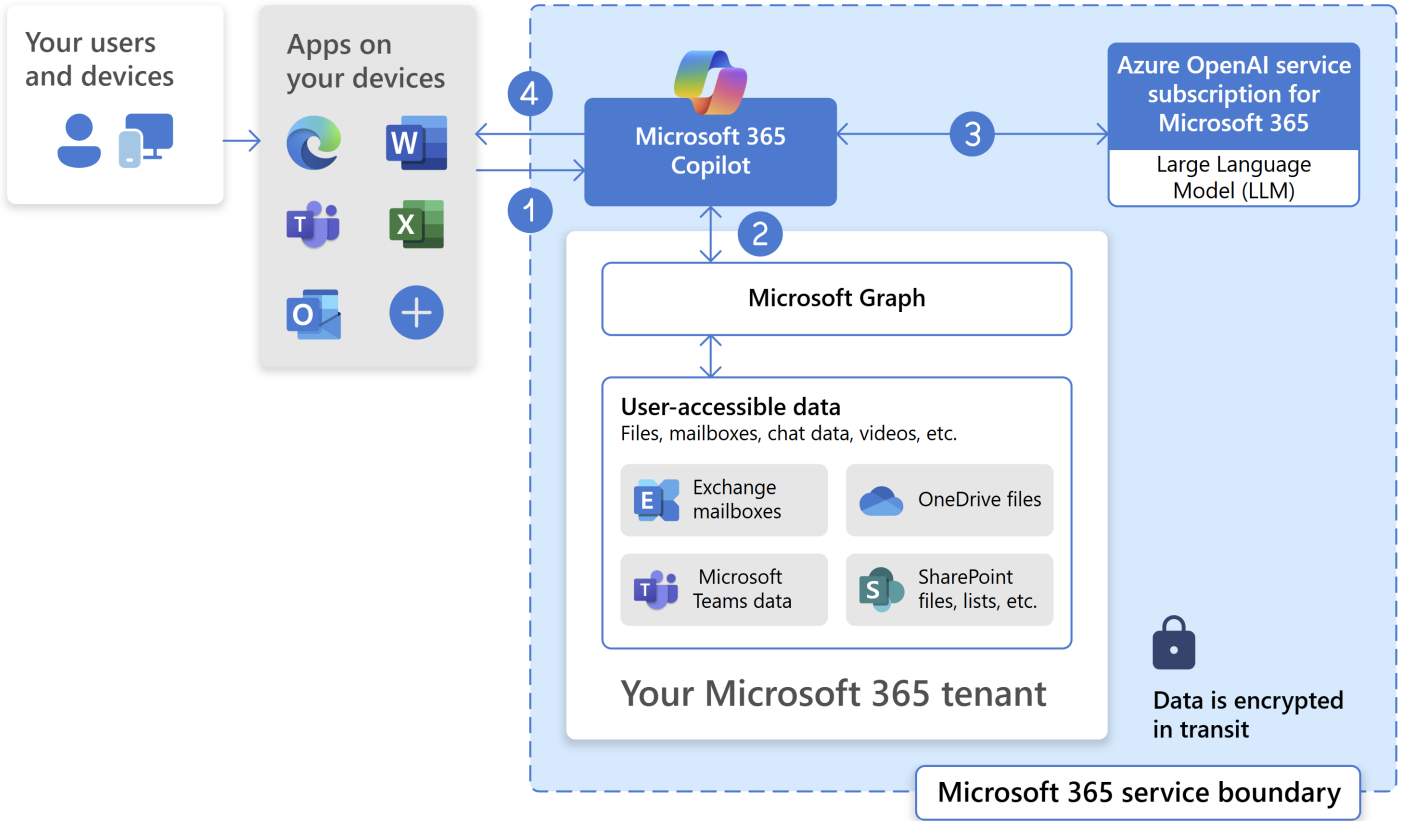


Azure OpenAI and API Management (APIM samples)

...ensuring everyone understands which regions data can travel to or can be processed in



Provide the customer with a detailed overview of data flow to illustrate how you work with data (example: copilot docs)



1. In a Microsoft 365 app, a user enters a prompt in Copilot.
2. Copilot preprocesses the input prompt using grounding and accesses Microsoft Graph in the user's tenant.
3. Copilot sends the grounded prompt to the LLM. The LLM uses the prompt to generate a response that is contextually relevant to the user's task.
4. Copilot returns the response to the app and the user.

Example 2: user access and data privacy

… and please mention Brad Smith’s announcement @ Atlantic Council (link)

Microsoft's new European digital commitments

1. We will help build a broad AI and cloud ecosystem across Europe.
2. We will uphold Europe’s digital resilience even when there is geopolitical volatility.
3. We will continue to protect the privacy of European data.
4. We will always help protect and defend Europe’s cybersecurity.
5. We will help strengthen Europe’s economic competitiveness, including for open source.

Clients talking compliance

Data protection considerations.

Question:

How can it be ensured when using AzureOpenAI that the data remains within a specified Azure region and is not transmitted to Open AI?
(see above, part of our commitment)

How can I technically deal with having customers in multiple regions with different location requirements? (Traffic from predefined vs unknown locations, Azure FrontDoor, …)

My customer asks for the tool to be deployed within their environment. How can I do this? (Managed Apps, Templates, Lighthouse , CI/CD considerations – aka maintenance)

Nordcloud
an IBM Company

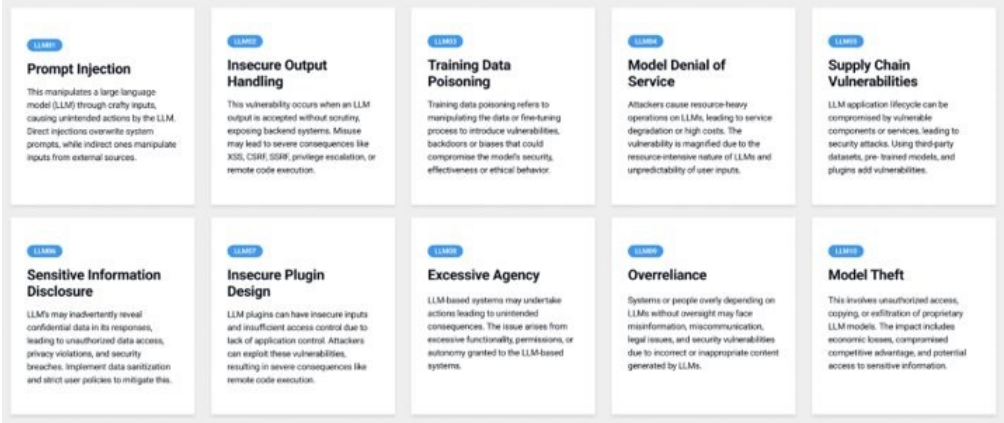
Clients talking compliance

Security considerations.

Question:

What technical measures should I consider to make sure that I cover the best practice security standards?

- Secure Application design
- Access controls
- Supply chain security
- Encryption
- For a broader best practice: SFI



Nordcloud
an IBM Company

Links

- Trust Centre
- Secure Future Initiative (SFI)
- Azure, Dynamics 365, Microsoft 365 and Power Plat compliance offerings
- Data, Privacy, and Security for Azure Open AI Service
- Service Trust Portal (certifications)
- Consolidated Compliance Resources
- Compliance assets for customers and partners