COMMERZBANK

A risk-based approach to Artificial Intelligence

a tour around Commerzbank's White Paper on the European Artificial Intelligence Act

Julia Sterling
Frankfurt, 18th April 2023

Join our AI Tour Bus:

1st Stop: AI @ Commerzbank

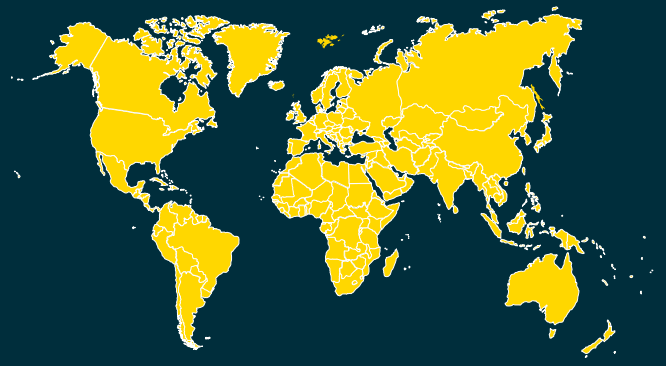
2nd Stop: Banking Perspective on EU AI Act

3rd Stop: Impacts on ML Governance

1st Stop: AI @ Commerzbank

Overview of Group Big Data & Advanced Analytics

>500 Colleagues in Germany & Abroad



in **4** Countries

We create value from data

~5 Years BDAA

7 Cluster

Value of AI @ Commerzbank

Areas	**Marketing & Revenue Growth**	**Risk Quantification**	**Loss & Fraud Prevention**	**Cost Reduction & Efficiency**
Examples	• Next Best Offer • Churn prevention	• Credit risk models • Market risk models • Portfolio models	• Early Warning Signals • Fraud Detection • Financial Crime Prevention	• Document analytics • Transaction data analytics
Impact	**Targeted Recommendations**	**Efficient Capital Allocation**	**Optimize Cost of Risk & Fraud**	**Process Automation**

AI & ML innovation comes with large opportunities as well as with risks which need to be addressed

- AI has the power to exceed capacities of traditional models by far (e.g. ability for autonomous decision making etc.)
- AI innovation leads to risk & return trade-offs, and successful AI and ML implementations must take the cost of risk mitigation into account.
- Among these are transparency vis-à-vis users, consistent performance of the systems etc.
- Using AI depends on the specifics of the situation:
  - Data quality and data linkages across different sources increase model results of traditional and ML models alike.
  - In some cases, simpler data-driven approaches or “classical” statistical methods can provide predictive power similar to more advanced AI & ML, but without some of the associated risks. Describing complex, non-linear relationships usually requires ML methods to be used.
  - Through AI/ML the effectiveness and efficiency of processes with human interaction can be increased while at the same time addressing risks.

2nd Stop: Banking Perspective on EU AI Act

AI definitions are very broad (I)

AI System according to Council's General Approach[1)]

"'*Artificial intelligence system' (AI system) means a system that is designed to operate with*

- ***elements of autonomy*** *and that,*
- *based on* ***machine and/or human-provided data and inputs****,*
- ***infers how to achieve a given set of objectives***
- *using machine learning and/or logic- and knowledge based approaches,*
- *and produces* ***system-generated outputs*** *such as content (generative AI systems), predictions, recommendations or decisions,*
- *influencing the environments with which the AI system interacts;"* (Article 3)

"*A system that uses rules defined solely by natural persons to automatically execute operations should not be considered an AI system*" (p.6 (6))

1) Reference based on the General approach of the Council of the European Union as of 6th December 2022 "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts". Please note that the definitions as all other passages of the AI Act will be subject to the trilogues be can still change.

AI definitions are very broad (II)

Machine Learning according to Council's General Approach[1)]

"Machine learning approaches focus on

- *the development of systems capable of learning and inferring from data*
- *to solve an application problem* ***without being explicitly programmed*** *with a set of step-by-step instructions from input to output.*

Learning refers to the ***computational process of optimizing from data the parameters of the model****, which is a mathematical construct generating an output based on input data."*

The range of problems addressed by machine learning typically involves tasks for which other approaches fail, either because there is no suitable formalisation of the problem, or because the resolution of the problem is intractable with non-learning approaches.

Machine learning approaches include for instance

- *supervised, unsupervised and reinforcement learning,*
- *using a variety of methods including deep learning with neural networks, statistical techniques for learning and inference (including for instance logistic regression, Bayesian estimation) and search and optimisation methods."* (as per p. 6 (6a)).

For a definition of Logic- and Knowledge Based Approaches please refer to p. 7 (6b).

1) Reference based on the General approach of the Council of the European Union as of 6th December 2022 "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts". Please note that the definitions as all other passages of the AI Act will be subject to the trilogues be can still change.

Risk-based approach

AI Risk Classes

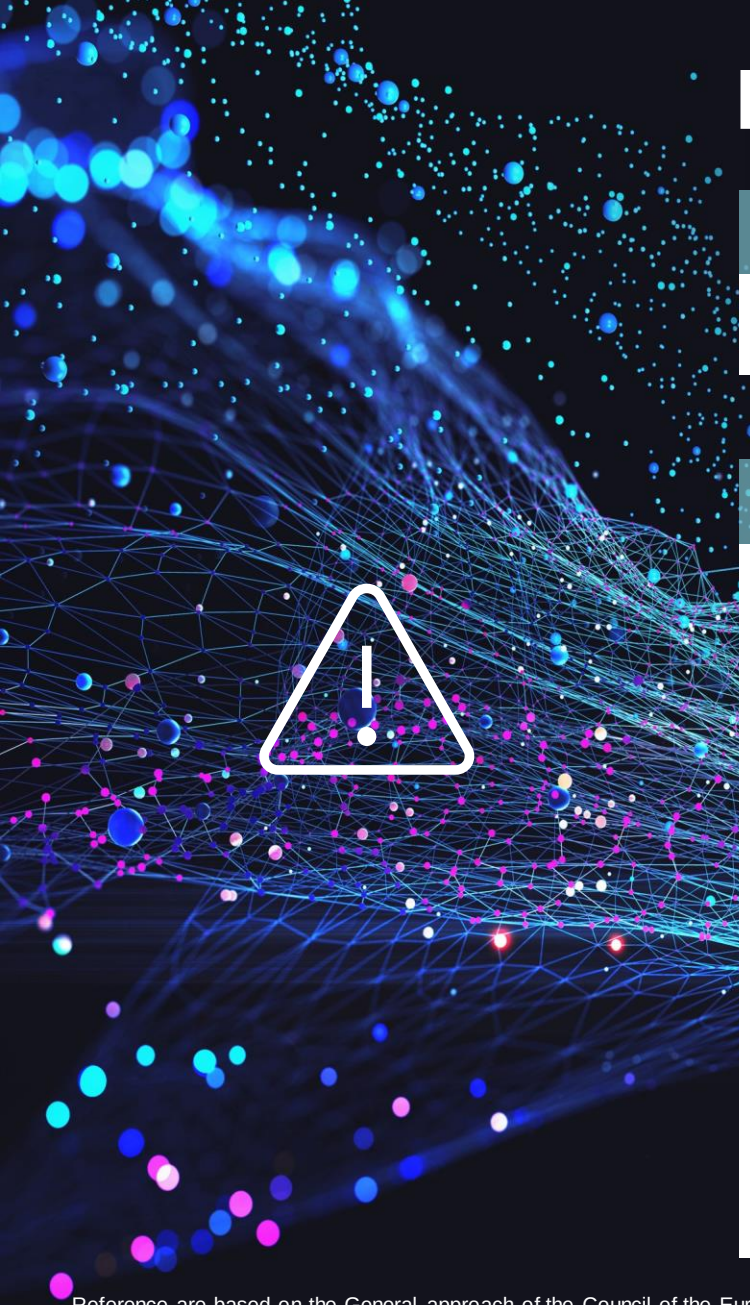
Commerzbank's risk-based approach covers model complexity, impact range and business criticality, resulting in the following risk categories:

- Prohibited AI Systems[1)]
- High-Risk AI Systems (according to AI Act Annex III or internally classified bank criticality)
- AI Systems with Transparency Obligations
- Low Risk AI Systems
- Ad-hoc Analysis
- No AI

1) Prohibited is using AI for manipulative, exploitative and social control practices. Further definitions and details can be found in Article 5 of the AI Act.

Reference are based on the General approach of the Council of the European Union as of 6th December 2022 "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts". Please note that the definitions as all other passages of the AI Act will be subject to the trilogues be can still change.

High-Risk AI Systems acc. to to AI Act



What is High Risk?

This is still under **a lot of debate within the EU** and therefore we are monitoring the developments closely.

Requirements of High-Risk Systems

In order to address and mitigate risks appropriately, high-risk AI systems (according to the AI Act) will have to comply with a set of horizontal mandatory requirements for trustworthy AI (Title III; chapter 2) and need to follow a conformity assessment procedure (Article 43) before they can be placed on the EU market. Moreover, they will be obliged to be registered in an EU database for high-risk AI Systems (Article 51).

Amongst others, the following requirements exist for high-risk AI systems that are listed according to Annex III of the AI Act:

- Risk Management System (Article 9),
- Data and data governance (Article 10),
- Technical documentation (Article 11),
- Record-keeping (Article 12),
- Transparency and provisions of information to users (Article 13),
- Human oversight (Article 14),
- Accuracy, robustness, and cybersecurity (Article 15).

Reference are based on the General approach of the Council of the European Union as of 6th December 2022 "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts". Please note that the definitions as all other passages of the AI Act will be subject to the trilogues be can still change.

Certification Requirements

Idea

Certificates and CE markings should **increase trust in the solutions** offered and consequently support and foster innovation.

Our Position

- **What exactly is certified?** → Certifications can only be point-in-time snapshot or back-wards oriented
- **Catalogues are not final** as this is an ever changing field, so hard to compare over time.
- There can be changes in the data over time or different results can occur in different situations. Hence whole process could be certified. Yet a **complex certificate cannot easily be understood by humans** and not establish trust as intended.
- Certificate is no **"carte blanche"** to use third-party software regardless of the situation
- **Responsibility can never be outsourced.** It is questionable to what extent banks can rely on this testimony or will need to perform the evaluations on their own. Hence, it must be determined how banks can use certifications. Being able to rely on these is especially important for efficiently implementing state-of-the-art **general purpose AI**.

Reference are based on the General approach of the Council of the European Union as of 6th December 2022 "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts". Please note that the definitions as all other passages of the AI Act will be subject to the trilogues be can still change.

In the jungle…

Regulatory Context

Developing, training, evaluation and deployment of AI systems needs to adhere to various requirements in addition to the upcoming AI Act. Like:

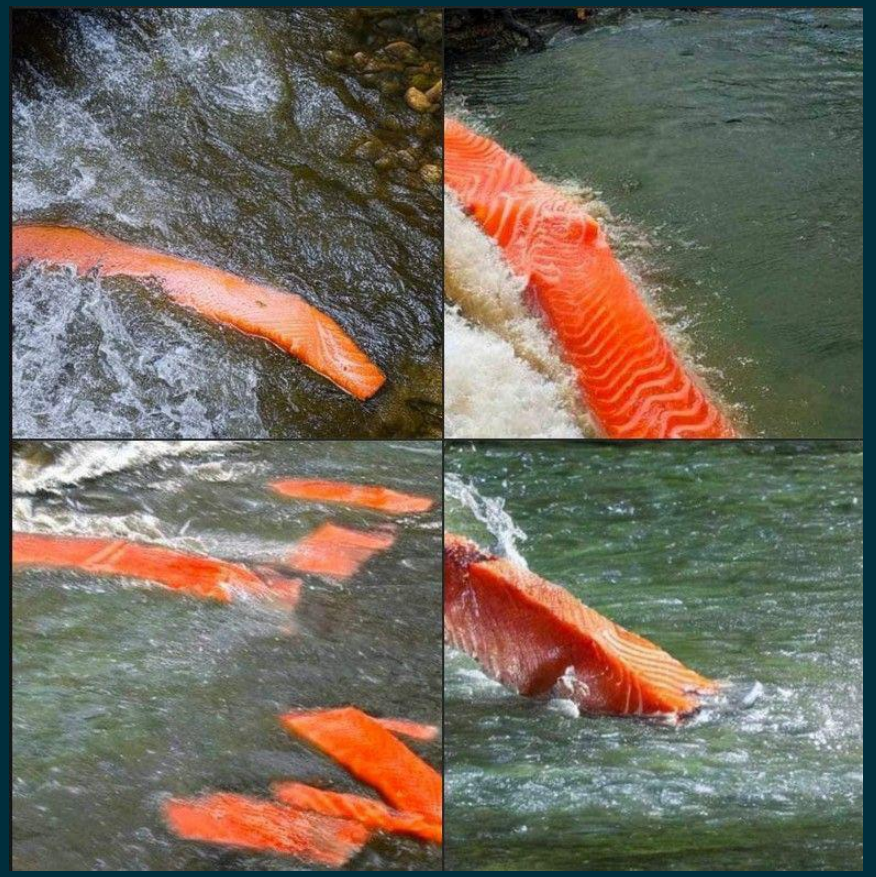
- Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms
- EU General Data Protection Regulation (GDPR)
- European Data Act
- European Data Governance Act
- Supervisory Requirements for IT in Financial Institutions (BAIT)
- Minimum Requirements for Risk Management (MaRisk)
- EBA Guidelines on outsourcing arrangements
- Digital Operational Resilience Act (DORA)
- EBA Guidelines on ICT and security risk management
- MiFID, esp. relevant for algorithmic trading
- At least indirectly through many more regulation like laws on worker and consumer protection, equality, anti-discrimination etc.

Due to the entanglements of Artificial Intelligence with various other regulations like GDPR we call for a coherent harmonization of rules.

3rd Stop: Impacts on ML Governance

Why take a closer look at AI & ML Governance? (I)

Example A: two different versions of AI Art imagining “salmons in the river”



Why take a closer look at AI & ML Governance? (II)

Example B: Correlation can but must not mean causality…

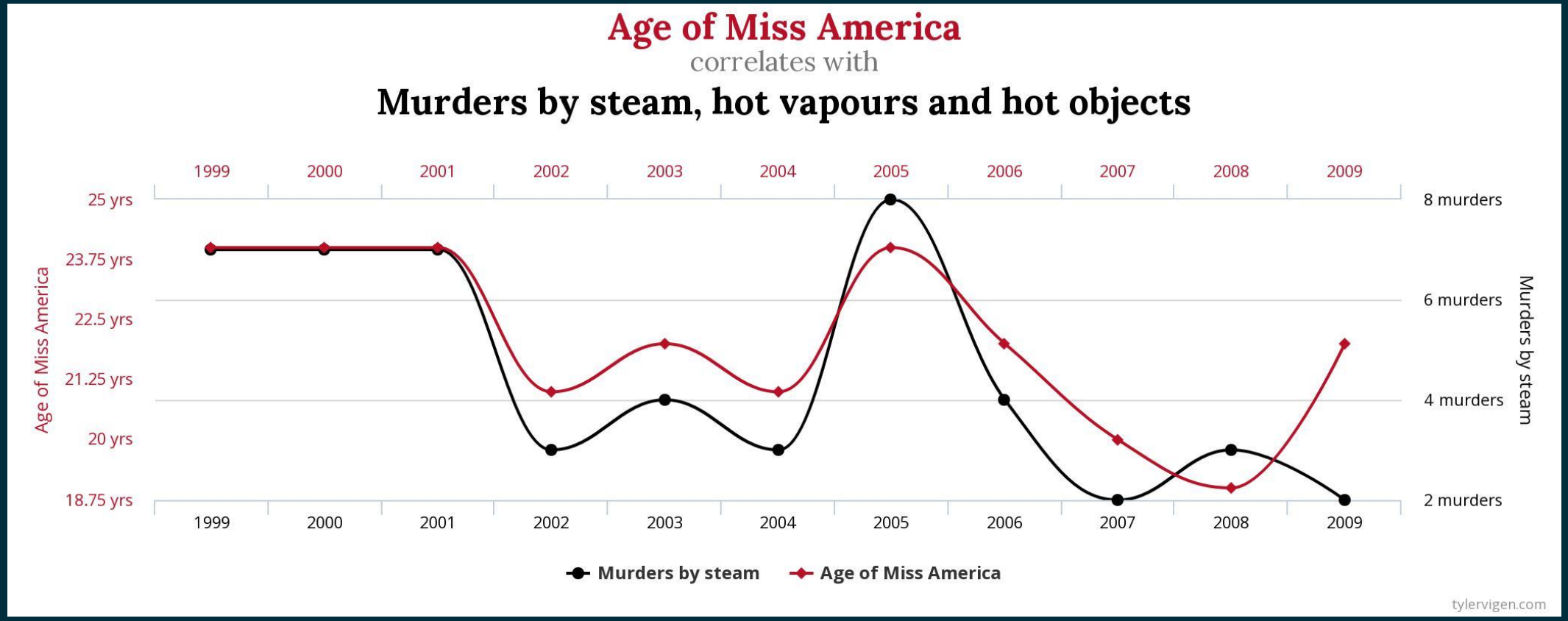
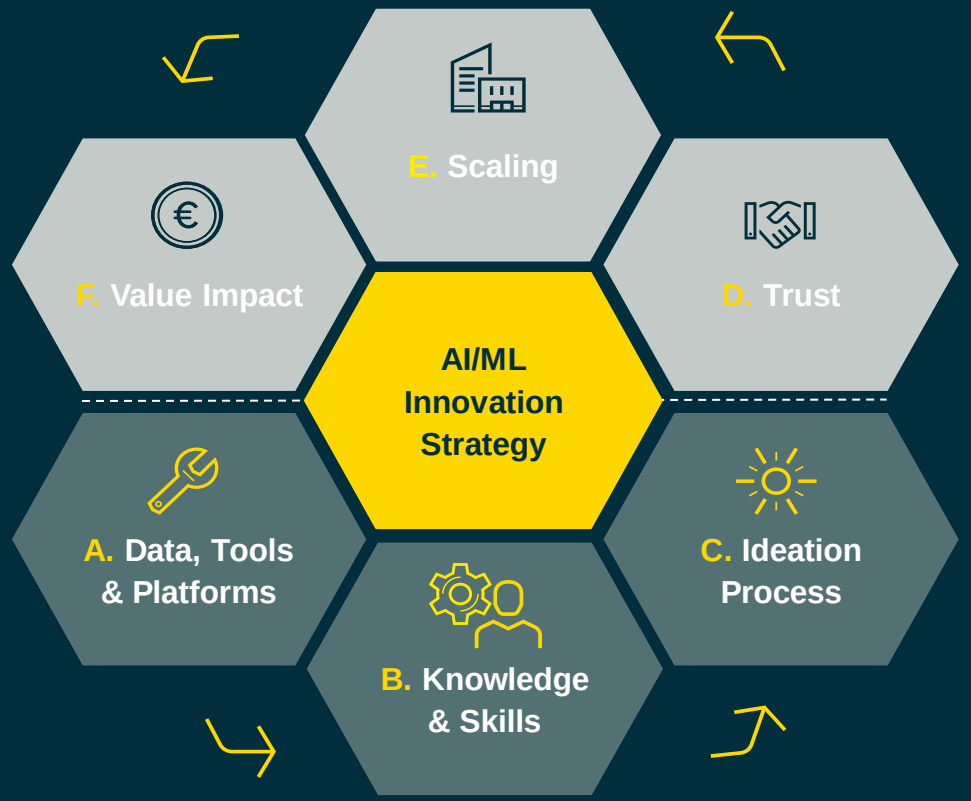


Chart from https://www.tylervigen.com/spurious-correlations (Last accessed 8th Sept 2022)

AI & ML Strategy needs to address risks by appropriate ML Governance

The basis for innovation and long-term success



Pillars of ML Governance

Center of Competence

Esp. for usage of AI/ML in core banking activities and involvement of external ML vendors

Three Lines of Defense for AI/ML

Leveraging on existing structures and following a risk-based approach

Handbook on Trustworthy AI

How to tackle, assess and mitigate AI/ML related risks

AI/ML Inventory

Enable scaling through transparency, derive advisory needs, risk-based assessment and reporting

Three most discussed AI Ethics Buzzwords in public[1)]

Transparency

- Transparency is about being clear, open, and honest about how and why a person's data is being used
- Spotlight on: Interdependency with GDPR

Explainability

- ranges from interpretability of input-output relations to the precise inner workings of models
- amounts to justifying the process from data and model selection to model validation and monitoring, thereby ensuring the control over its intended use.
- Spotlight on:
  - Addressee and Context
  - Overreliance

Fairness

- Bias from algorithms describes a situation where there is a wrongful discriminatory judgement encoded into an algorithm.
- Since ML models learn patterns from past data, they "learn" biases prevailing in the data through correlation.
- Spotlight on:
  - Correlation vs. Causality
  - Discrimination vs. Differentiation
  - How does discrimination enter the algorithm?
  - Is fairness always unambiguous?

[1)] There are many aspects to consider when defining Trustworthy and Responsible AI. Most of these concepts are already well known and standard procedure when bringing software into production or processing data in general (cf. Prudential Requirements for IT (BAIT), General Data Protection Regulation (GDPR) etc.).

White Paper Released Feb 15th 2023

Thank you for your time!

Julia Sterling

Vice President
Business Development
Big Data & Advanced Analytics

Telefon +49 69 136 – 811 36

julia.sterling@commerzbank.com

Geschäftsräume:
Neue Börsenstraße 1,
60487 Frankfurt am Main
www.commerzbank.de

Postanschrift:
Neue Börsenstraße 1,
60487 Frankfurt am Main