Data & AI Governance

August 27, 2021
Schweizer IT-Juristinnen Tag 2021

Elisabeth Bechtold
Global Lead Data Governance & Oversight
Zurich Insurance Group

Agenda

1. What's the challenge?
2. Trust in a data-driven world
3. Managing data and AI risk
4. Establishing an AI governance framework
5. Appendix: Zurich's Data Commitment

What’s the challenge?

Challenges in a data-driven world

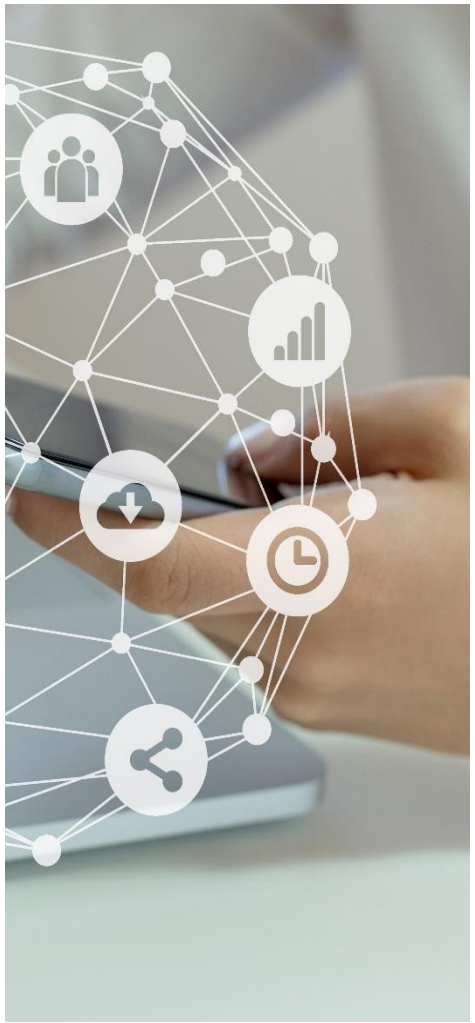
CHALLENGE

- Data is getting increasingly relevant for both our professional and private lives
  - COVID-19 crisis as an accelerator of digital transformation and focus on data
- Opportunities, challenges and concerns in a data-driven world are equally on the rise
- What does this mean for corporations?
  - Implications, risks – and opportunities?

- Key dimensions of data and AI risk:
  - IT & Cyber Security
  - Data & Information Governance
  - Responsible use of data, including use of algorithmic decision-making such as machine learning (ML) and artificial intelligence (AI)

OPPORTUNITY

- Promoting the responsible, human-centric and beneficial use of data and advanced technologies such as AI for the benefit of customers and society at large
- Inspiring trust in a digital society



AI & ethics

Trust in a data-driven world

Inspiring trust through sound data governance

ZURICH

Data is key for business success … and requires sound governance to establish customer trust.

- Customers must trust companies they share their data with (custody)
- Companies must appropriately govern the use of data, including in the context of algorithmic decision-making such as AI
- Customers must trust companies on the way they use and govern data

Ethical AI – policy trends and emerging regulation

Policy

- Global **public policy debate on ethical use of AI:**
  - National AI strategies
  - Best practices and emerging regulation
- **EU** builds on GDPR momentum and takes on **thought leadership on ethical AI**
  - **European Commission** published **legislative proposal on trustworthy AI in April 2021,** pursuing a risk-based approach
- **U.S.** is increasing its **regulatory focus on AI,** likely influenced by progressive EU approach
- **China** is establishing a comprehensive **legal, ethical, and regulatory framework for AI by 2030**
- **Russia** starts engaging in international policy discourse on ethical AI

While binding regulation is underway, a global consensus around five principles on ethical AI has crystallized …

Proposed EU Artificial Intelligence Act

STATUS

- On April 21, 2021, the EU Commission proposed a **horizontal regulatory framework that encompasses any AI system that touches the single market** (whether the provider or distributor is based in the European Union or not).
- The European Parliament and the Member States will need to adopt the Commission's proposal in the ordinary legislative procedure. Once adopted, the regulation will **directly apply across Member States**.

KEY POINTS

- The **Artificial Intelligence Act** (AIA) pursues a **risk-based approach** and sets up a series of escalating legal and technical obligations depending on whether the AI product or service is classed as low, medium or high-risk, while specific of AI uses are banned outright.
- The proposed legislation is notable for its **expansive definition of AI systems**, and the imposition of **extensive documentation, training, and monitoring requirements on AI systems** that fall under its purview.
- **AIA will apply extraterritorially to any provider or distributor of AI whose services or products reach the EU market**. This includes providers and users of AI systems outside the EU if the output of the AI system is used in the EU.
- The **AIA defines AI broadly** as a suite of software development frameworks that encompass **machine learning, expert and logic systems, and Bayesian or statistical approaches**. A software product featuring these approaches whose outputs "influence the environments they interact with" will be covered.
- The AIA distinguishes three categories of AI systems:
  - **Prohibited AI applications**
  - **High-risk AI uses**
  - **Low-risk AI systems**

Proposed EU risk classification of AI systems

Unacceptable-risk AI systems

- Subliminal, manipulative, or exploitative techniques causing harm
- Real-time, remote biometric identification systems used in public spaces for law enforcement
- All forms of social scoring

High-risk AI systems

- Systems that evaluate consumer creditworthiness
- Recruiting or employee-management systems
- Systems utilizing biometric identification in nonpublic spaces
- Safety-critical systems (eg, systems that would put the health of citizens at risk due to failure)
- Any systems used in the administration of justice

Limited- and minimal-risk AI systems

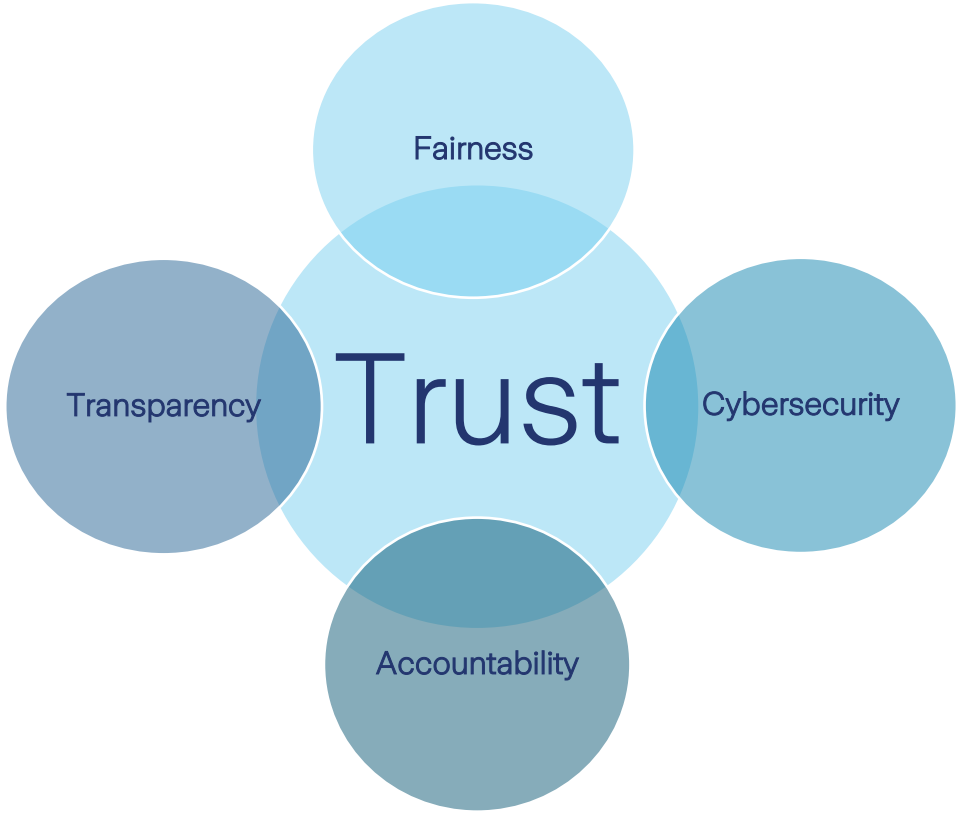
- AI chatbots
- AI-enabled video and computer games
- Spam filters
- Inventory-management systems
- Customer- and market-segmentation systems
- Most other AI systems

Source: McKinsey, What the Draft European Union AI regulation means for business

What does the proposed AI legislation mean for businesses?

The proposed AIA defines comprehensive **governance requirements** on organizations providing or using high-risk AI systems:

- Implementation of an AI risk management system
- Data governance and management
- Technical documentation
- Record keeping and logging
- Transparency and provision of information to users
- Human oversight
- Accuracy, robustness, and cybersecurity
- Conformity assessment
- Registration with with EU-member state government
- Post-market monitoring



For **medium- or low-risk AI systems**, organizations are also encouraged to pursue a **robust governance and risk management approach** to ensure AI applications perform as intended along an AI system's life-cycle with a focus on **fairness**, **transparency**, **accountability**, and **cybersecurity**.

Managing data & AI risk

AI risk dimensions

REPUTATIONAL, REGULATORY & LIABILITY RISK

Reputational risk

- Inappropriate (biased) outcome

Regulatory risk

- GDPR fines
- Unlawful discrimination

Liability risk

- Harm caused by AI/ML systems
- Complications by third parties

AI-SPECIFIC RISK DIMENSIONS

Lack of transparency

- Explainable AI

Complex models

- Governance challenges

Ethical challenges

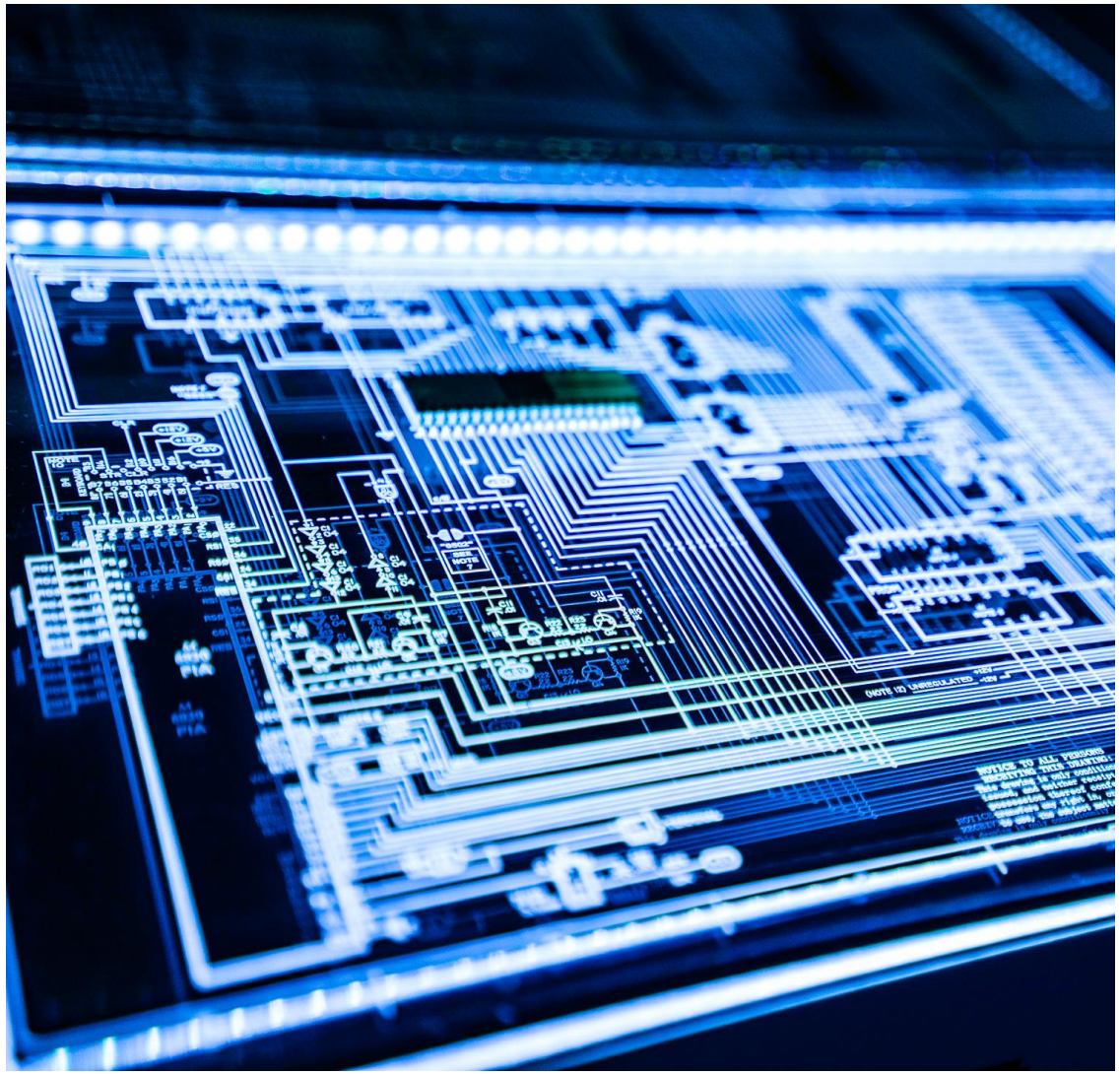
Example: Insurance

- Risk selection & pricing
- Underwriting

Penalties for infringement proposed by EU Artificial Intelligence Act

The EU Commission expects Member States to lay down **effective, proportionate and dissuasive penalties for infringements of the AI Act** and sets out the following thresholds:

- Up to **EUR 30m or 6% of the total worldwide annual turnover** of the preceding financial year (whichever is higher) for infringements on prohibited practices or non-compliance related to requirements on data;
- Up to **EUR 20m or 4% of the total worldwide annual turnover** of the preceding financial year for non-compliance with any of the other requirements or obligations of the AI Act;
- Up to **EUR 10m or 2% of the total worldwide annual turnover** of the preceding financial year for the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request.



Key challenges of AI liability (1/2)

Determining legal liability for AI systems faces 3 key challenges:

- Multiple contributors typically involved in the creation and operation of an AI system complicate causality
- Nature and cause of damage created by an AI system may be difficult to identify … but can be decisive for establishing and allocating liability
- Patchwork of potentially applicable generic legal concepts (e.g., product liability law, tort law, contract law, data protection & privacy law) and emerging set of specific rules for trustworthy AI

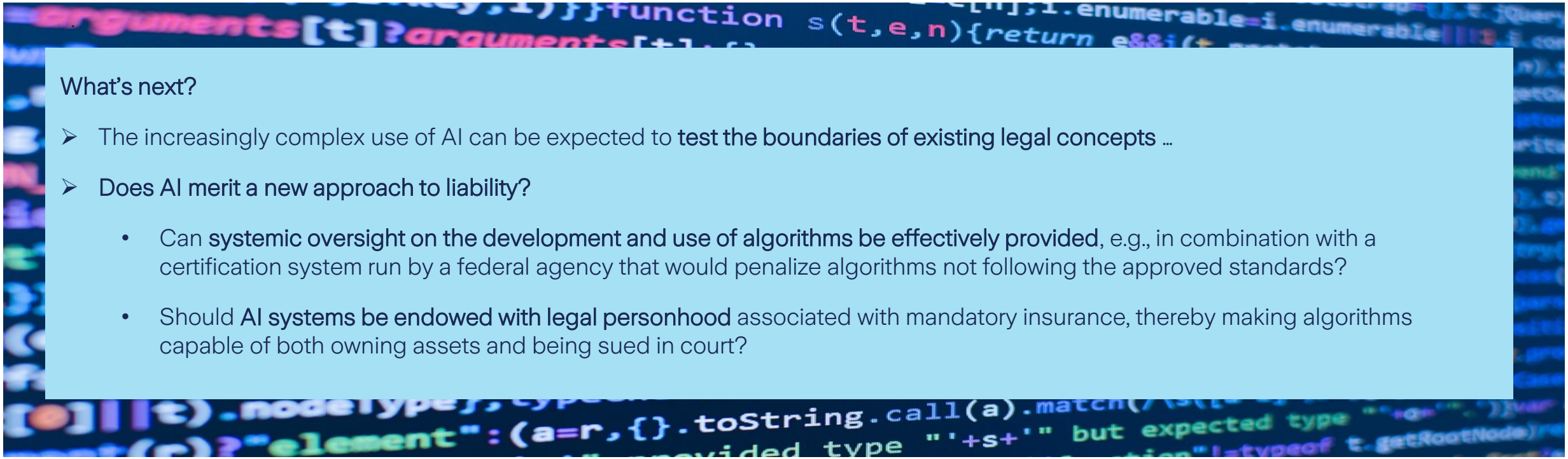
Nature or cause of damage	Who is liable?
Was damage caused when in use and were the instructions followed? Was the AI system provided with any general or specific limitations and were they communicated to the purchaser?	User or owner?
Was the damage caused while the AI system was still learning?	AI developer or data provider?
Was the AI system provided with open-source software?	Programmer?
Can the damage be traced back to the design or production of the AI system, or was there an error in the implementation by its user?	AI developer or user?

Source: CMS, Who is liable if AI fails to perform?

Key challenges of AI liability (2/2)

What are the key challenges and limitations of existing legal approaches?

- Based on existing legal mechanisms provided by tort and product liability law, in particular, complications may arise due to AI-specific features such as an AI's autonomy, its frequent appearance as a "service" (thus not subject to product liability laws), potentially multi-layered third-party involvement and the interface between humans and AI.



What's next?

- The increasingly complex use of AI can be expected to **test the boundaries of existing legal concepts** …
- **Does AI merit a new approach to liability?**
  - Can **systemic oversight on the development and use of algorithms be effectively provided**, e.g., in combination with a certification system run by a federal agency that would penalize algorithms not following the approved standards?
  - Should **AI systems be endowed with legal personhood** associated with mandatory insurance, thereby making algorithms capable of both owning assets and being sued in court?

For more information on algorithmic liability risk, see White Paper on Algorithmic Liability , co-authored by Zurich and Microsoft (July 2021)

Overview of selected AI risks

AI risks can materialize at all stages … but controls can mitigate them

CONCEPTUALIZATION RISK

- Potentially unethical use cases
- Insufficient learning feedback loop
  - ➢ Establish and monitor data & analytics risk principles

DATA RISK

- Incomplete or inaccurate data, insufficient data protection
- Other regulatory non-compliance
  - ➢ Define data quality metrics & provide assurance

MODEL DESIGN & IMPLEMENTATION RISK

- Non-representative data, biased or discriminatory model outcomes, model instability, implementation failures
  - ➢ Monitor adherence to transparency / explainability, fairness principles and proper implementation

PERFORMANCE RISK

- Poor model performance, cyber security threats
  - ➢ Monitor access management, performance, cyber protections / resilience, capture and analyze errors and other failures

Establishing AI governance

Align corporate values with responsible use of AI

In a first step, corporate values need to be translated into a common understanding of the ethical use of AI …

Relevant questions include:

How do values translate into the selection & deployment of AI applications?	… and is this position aligned with our stakeholders' expectations?
Which guidance is needed for evaluating AI for bias, fairness, etc.?	Are data sets representative and unbiased? When and where to consider fairness?
How to ensure adherence to ethical AI principles?	Are compliance and risk controls effectively built in our AI workflows?

Key governance considerations for establishing trustworthy AI

AI governance model

- Establish AI design methods, policies and standards for development and deployment of AI, including conduct and design principles
- Define AI governance and accountability mechanisms, ensure compliance with laws & regulations, and provide assurance

Independent audits

- Independent audit on ethical AI and design taking into account internal policies & standards as well as external standards and obligations to enhance user's trust in AI

AI controls

- Provide for inventory of algorithms (based on software discovery tools)
- Assess impact and risks of relevant algorithms (development and use)

Change management & communications

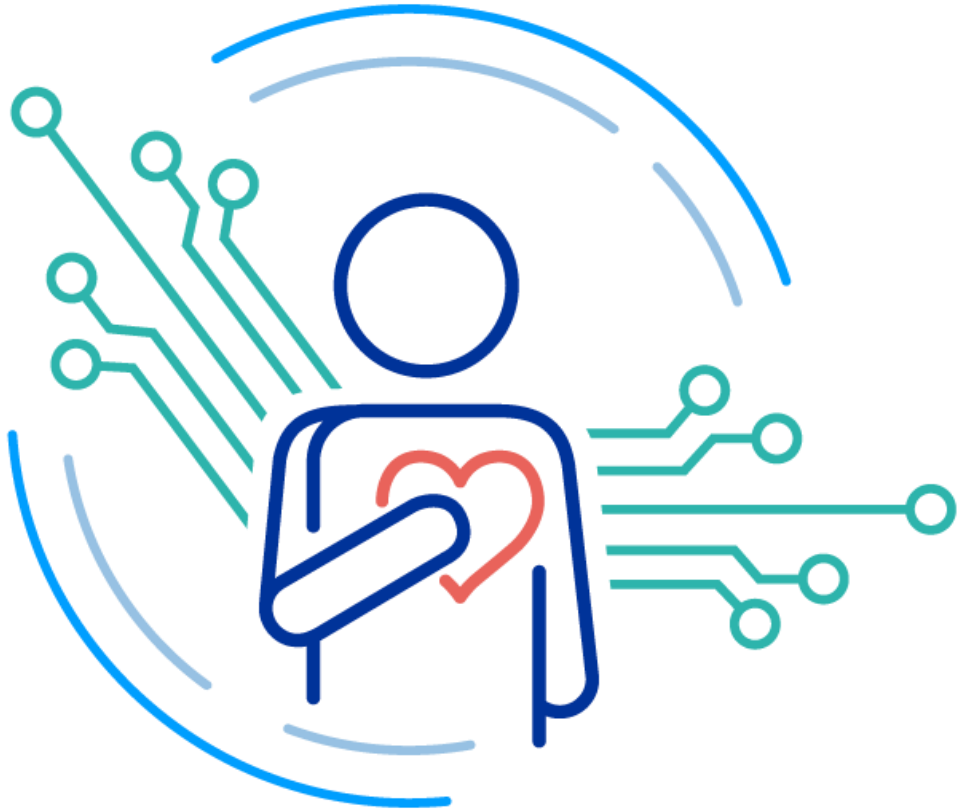
- Educate executives and developers of AI on the ethical considerations of AI and their responsibility to safeguard impacted users
- Provide for effective training and communications

Monitoring & validation

- Ensure algorithms are performing as intended and are producing accurate, fair and unbiased outcomes
- Monitor potential changes to algorithmic models

Such internal governance framework can be complemented with an advisory body composed of diverse, multi-disciplinary experts providing independent advice and strategic guidance on the ethical use of AI to the board of directors.

Focus on customer benefit and trust



Customer trust at the heart of business

Responsible use of data & technology

It is the responsibility of every company to be responsible stewards of data and technology for its customers

Focus on customer benefit and trust

The use of customer data is a valuable source to design better products and services, inspired by customer benefit and trust

Enabling resilient digital services

As business and life turns digital, all customer interactions must be secure, seamless, and always-on

Appendix

Zurich Data Commitment

Our objective is to enhance your experience when interacting with us and to develop innovative products and services that meet your overall needs and expectations.

Our commitment is underpinned by a set of **KEY PRINCIPLES** applied globally and adhered to by all Zurich employees.

The four promises made to our customers in Zurich's data pledge are to:

- Keep their data safe;
- Never sell their personal data;
- Not share their personal data without being transparent about it;
- Put their data to work so Zurich can better protect them, and so they can get the most out of life.

Thank you!

Please note that this presentation reflects the personal view of the author and not necessarily that of Zurich Insurance Group.