APRIL 2024

inside zhero

EU AI ACT
Europe leads the way

ZHERO GOES WEST
#EmpowerFrisco

EXEC TEAM
Welcomes Natasha!

Message from Izak

Great to see you all again and good to be back on home soil. A bit more about that later in this edition of Inside Zhero.

This month we're looking at AI risk management and regulatory compliance.

In this issue

Our feature "Act on AI" shows us how the EU AI Act will help us effectively govern AI-powered systems and manage risk.

Only 9% of companies are prepared to manage the risk produced by AI.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

“UK businesses need to put in place cybersecurity to cover people, processes and technology controls, including AI regulation and compliance, to shore up their overall cyber defences."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling author

Available Now

The Exec team welcomes Natasha!

Last month, our Head of Finance, Natasha Botha, officially became part of the Zhero Executive Team. Natasha joined the company in June 2020 to assist with accounts receivable. She quickly reaped the rewards of her expertise, level of commitment, and passion for Excel, and within six months was promoted to her leadership role. In Izak's words:

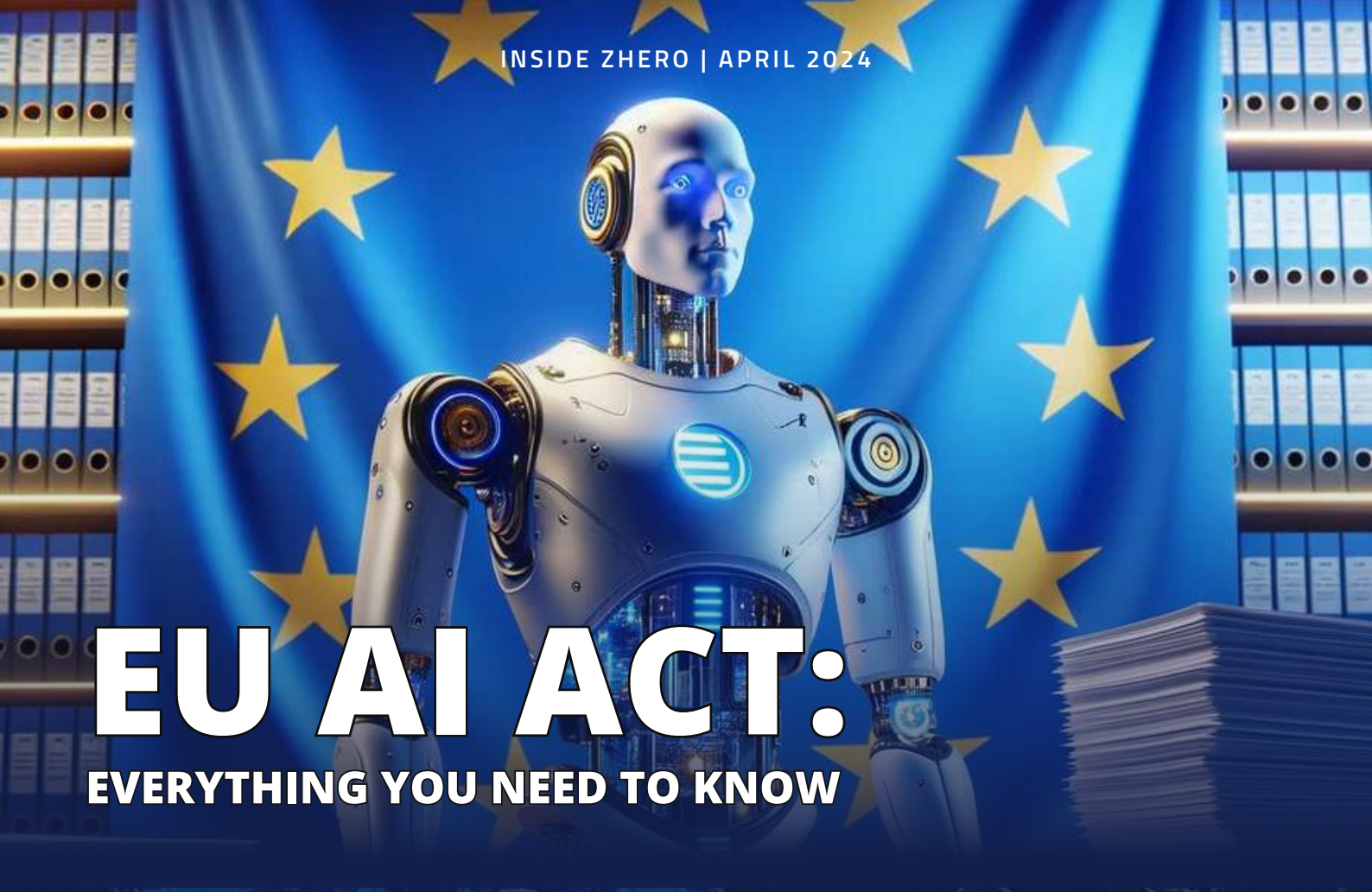
"Natasha is not just exceptional in her work but someone who always goes the extra mile, leading by example with the company's best interests at heart. She is an inspiration to all of us!"

Natasha finds fulfilment in strategizing and setting clear objectives, then guiding her team through the process of achieving them. Witnessing their professional and personal growth is incredibly rewarding for her.

Natasha also values the chance to foster a positive work environment where collaboration, innovation, and mutual respect thrive.

Team Zhero congratulates Natasha on her new position and knows that under her leadership we'll surely be going places! And here's a playful endnote from Izak:

"When she says we need to jump we all jump."



EU AI ACT:

EVERYTHING YOU NEED TO KNOW

The AI revolution descended upon us fast and furious last year, with a particular focus on generative technologies and Large Language Models (LLMs) like ChatGPT and Microsoft Copilot. Along with the hype, came warnings of the possible threats of AI, claiming that it could be both friend and foe. Here are two:

"There is some chance, above zero, that AI will kill us all. I think it's slow but there is some chance." ~ Elon Musk, Tesla CEO

"*These things could get more intelligent than us and could decide to take over, and we need to worry now about how we prevent that happening.*" ~ Geoffrey Hinton, the Godfather of AI

Hinton was so worried about his trailblazing developments on tools like ChatGPT, that he quit his job at Google after a 10-year stint. Musk joined forces with more than 1,000 other tech experts in a 2023 public statement advocating for a halt to extensive AI experimentation. Their collective concern stemmed from the belief that AI carries significant risks to humanity.

Threats and risks

While a takeover by AI as suggested by Hinton is a far-fetched notion, many cyber experts in the know acknowledge these threats and risks:

- automation-spurred job loss
- deepfakes
- privacy violations
- algorithmic bias caused by bad data
- socioeconomic inequality
- market volatility
- weapons automatization
- uncontrollable self-aware AI

Weapons automatization might be reserved for the likes of bad actors but some of these dangers apply directly to businesses, particularly those that want their AI systems to comply with regulations and standards.

AI and privacy

A central issue in AI regulation is privacy – safeguarding personal data that AI systems collect, process, and store. The extensive and continuous data collection enabled by AI poses a risk of exposing sensitive information.

AI tools can also infer sensitive details from apparently harmless data, something called predictive harm. Complex algorithms and machine learning (ML) models can discern personal attributes like sexual orientation, political beliefs, or health status from seemingly unrelated data. Group privacy presents another significant concern.

AI's ability to scrutinize and detect patterns within vast datasets may lead to the stereotyping of certain groups, potentially resulting in algorithmic discrimination and bias. These privacy challenges mean that businesses need to implement overarching legal, ethical, and technological measures to safeguard individual privacy.

Facebook scandal

In the 2010s political consulting firm Cambridge Analytica gathered data from more than 87 million Facebook users without their explicit consent, utilising a seemingly harmless personality quiz app.

This data was used to construct intricate psychological profiles of the users, then exploited to tailor personalised political advertisements during the 2016 Presidential Election in the United States. This incident showed us the capability of AI to deduce sensitive information, such as political views, from seemingly harmless innocuous data, like Facebook likes.

Facebook blatantly shunned the law and privacy regulations and paid a high price for its AI non-compliance. The scandal shocked the world and in 2018, $100 billion was knocked off from Facebook's market capitalisation.

AI compliance

AI compliance is exactly what it says on the tin. It's a process aimed at making that AI-powered systems adhere to all relevant laws and regulations. It also ensures that the data utilised to train AI systems is gathered and used lawfully and ethically. AI compliance also guarantees that AI-powered systems do not discriminate against any specific group or individual and are not employed to manipulate or deceive individuals in any capacity. It must not intrude upon individuals' privacy or cause harm to them in any form. Ultimately, AI compliance is about ensuring that AI-powered systems are deployed responsibly and in a manner that contributes positively to society.

Why is it important?

- AI compliance guarantees that we use AI in a manner that aligns with legal and ethical standards.
- It's also a protective measure for businesses against potential legal and financial liabilities.
- Last but not least, AI compliance plays a vital role in safeguarding the privacy and security of individuals.

Entering the playground

Nearly three years after the first proposal, the EU Artificial Intelligence Act was approved by the European Parliament on 13 March, with 523 votes for and 46 votes against. The Act, paving the way for compliance, represents a first-of-kind AI regulation, classifying risk as:

- Applications and systems that pose an unacceptable risk, such as government-operated social scoring akin to practices in China, are prohibited.
- High-risk applications, like CV-scanning tools used for job applicant ranking, are subjected to stringent legal obligations.
- Applications not categorised as high-risk or explicitly banned are predominantly left unregulated.

"Today is again a historic day on our long path towards regulation of AI. The first regulation in the world that is putting a clear path towards a safe and human-centric development of AI."

BRANDO BENIFEI - MEMBER OF EUROPEAN PARLIAMENT

What does the Act propose?

According to the European Commission, the legislation will:

- address risks specifically created by AI applications.
- prohibit AI practices that pose unacceptable risks.
- determine a list of high-risk applications.
- set clear requirements for AI systems intended for high-risk applications.
- define specific obligations for deployers and providers of high-risk AI applications.
- require conformity assessment before an AI system is put into service or placed on the market.
- implement enforcement mechanisms after an AI system is placed on the market.
- establish a governance structure at both European and national levels.

What about the UK?

City A.M. tells us that the EU AI Act will probably exert a considerable influence on UK businesses, as adhering to it is essential for those engaging in international business. Any UK business selling AI systems in the European market or deploying AI systems within the bloc will be subject to its provisions. Forrester principal analyst, Enza Iannopollo, elaborated:

"Over time, at least some of the work UK firms undertake to be compliant with the EU AI Act will become part of their overall AI governance strategy, regardless of UK specific requirements – or lack thereof."

Levels of risk

You can see that the EU AI Act hones in on risk. These are the four levels of risk defined by the regulatory framework:

- **Unacceptable** - the use of applications with subliminal techniques, exploitative systems, or social scoring systems by public authorities is strictly forbidden.
- **High** – these include applications in transport, education, employment, and welfare and before bringing a high-risk AI system to market, companies are required to undergo a comprehensive “conformity assessment”
- **Limited** – these refer to the potential risks from the lack of transparency in the utilisation of AI. For example, when we use AI systems like chatbots, we should be informed that we are interacting with a machine, enabling us to make informed decisions about whether to proceed or disengage.
- **Minimal** - these include applications like AI-enabled video games or spam filters and most AI systems currently used in the UK are minimal risk.

AI Act versus GDPR

How does the EU AI Act compare with the GDPR? A simplistic comparison would be that the Act focuses on machines and risk while the GDPR is all about our data and privacy. More specifically, while both regulate the use of technology in the EU, the AI Act has a narrower focus on high-risk artificial intelligence specifically, imposing stricter rules and oversight for those systems. GDPR has a much broader scope covering all data processing and personal data.

Compliance and penalities

- **Compliance** - the AI Act proposes a conformity assessment and certification process for high-risk AI systems. GDPR does not have any certification requirements.
- **Penalties** - the AI Act proposes fines of up to €30 million or 6% of global turnover for non-compliance. GDPR fines can go as high as €20 million or 4% of global turnover.

Development heads WEST

Last month, our development team (Izak, Wesley Harris, Zhero's Head of Development, and Louis Oosthuizen, our Developer), headed Stateside to attend the N-able Empower event at the Omni PGA Frisco Resort in Texas. The conference, headlined as 'Forward Never Stops', brought together experts from around the world to exchange ideas on strategies and best practices across automation, backup, business, monitoring, operations, and security. Sponsors included Halopsa, Microsoft, ThreatLocker and more.

Izak and Louis were invited by N-able as guest speakers. Izak shared his expertise on cybersecurity standardisation, highlighting the five essential security practices that all businesses should have in place as laid out in his bestseller, 'You Don't Need a £1Million Cybersecurity Budget'. He also spoke of both his journey in IT and that of Zhero, explaining how the company has adopted the Rockefeller Habits as a framework for scaling up. Louis presented on cloud migration and how Cloud Commander helps MSPs overcome many challenges which they face when implementing this new frontier.

We spoke with the team to get their feedback on the event. This is what they had to say!

"Empower was the best! World Class!" - Izak

Wesley says – "An eye-opening experience. All IT companies are facing the same issues in cybersecurity today but there is a very big push to leverage AI tools to solve them."

In Louis' words – "Empower was astounding. Seeing so many partners collaborate and how to use N-able products to engage with daily tasks was inspiring."

Besides discovering the latest IT monitoring and management tools at Empower, Izak, Louis, and Wesley also had time out to sample delicious Texas BBQ and see the sites of Dallas.

Before jetting back home, the three took a bite out of the Big Apple, exploring Central Park, Broadway, the Empire State Building and the Statue of Liberty. The big question is where will they end up next?

EU AI ACT & GDPR: THE IMPACT ON YOUR BUSINESS

MARK CHILD
Quantum-Evolve

JAMIE CHAMBERLAIN
Zhero

15 May 2024 | 10:00 AM BST

We are on the cusp of a whole new world driven by technological advances in Artificial Intelligence (AI). Used wisely, AI may become our most powerful productivity tool. Unfortunately, the technology also comes with many potential risks and threats. The GDPR, focused on data protection and privacy, cannot adequately regulate AI and machine learning (ML). To mitigate these risks, the EU AI Act was passed in March this year, aiming to establish a common regulatory and legal framework for AI.

Join Jamie Chamberlain and cybersecurity expert Mark Child, Founder of Quantum Evolve for an hour of insight into this fledgling and first-of-kind AI Act. In a lively and interactive discussion in which they will cover what the EU AI is all about and its synergy with the GDPR. Mark will also show us how this regulation addresses the risks associated with machine-powered systems and what the Act means for companies developing and deploying AI.

Reserve your spot!

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

Meet the team

Natasha Botha

HEAD OF FINANCE

Hi Natasha! What made you realise you want to go into the IT industry?

I didn't choose IT, IT found me, and ever since it's been challenging me on various levels which kept me intrigued.

What's your most-used productivity tool?

Excel and Chat GPT – what's not to love about spreadsheets and AI!

How would you describe yourself?

I am results-oriented and pride myself on being a proactive problem-solver, addressing challenges head-on and finding solutions for everybody.

What do you enjoy the most about your role?

The opportunity to lead and develop a team of talented individuals. Being able to inspire and empower my team members to reach their full potential brings me immense satisfaction.

Do you have any hidden talents or hobbies?

I love cooking, whether it's a talent, I'm not sure, but it's definitely a hobby.

What is your favourite movie or TV show?

Not much of a bencher, but my all-time favourites are Law and Order SVU and Pretty Woman.

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

zhero
crush the chaos