



Privacy-Enhancing Computation: A Paradigm Shift in Data Privacy and Utility

Dr. Bertalan Forstner
Emerging Technologies Strategist
bertalan.forstner@zenitech.co.uk

February 2025

CONTENTS

Introduction	3
What is privacy-enhancing computation and why now?	6
The business benefits of PEC	7
The technical landscape of PEC	10
Key considerations for businesses	11
What should businesses do today?	14
Concrete applications of PEC	15
So what to do next	18



Introduction

In the evolving digital landscape, privacy is no longer an abstract concern, but a tangible challenge demanding innovative solutions. Privacy-Enhancing Computation (PEC) is one of the most promising technologies shaping the future of secure data usage. By enabling organisations to harness the value of data without compromising confidentiality, PEC stands at the crossroads of necessity and opportunity.

At its core, PEC allows computations on sensitive data without exposing the raw inputs. This is achieved through sophisticated methods - such as homomorphic encryption, secure multi-party computation, and differential privacy. Each approach is engineered to address specific privacy concerns while maintaining data usability. Yet, PEC is not merely a technical advancement – **it represents a shift in how industries approach data collaboration, regulation compliance, and customer trust.**





What is privacy-enhancing computation and why now?

The concept of privacy-enhancing computation isn't new, but its relevance has surged due to the exponential growth in data generation and the increasing severity of data breaches. From GDPR in Europe to CCPA in California, global regulations emphasise data protection, and organisations are compelled to adapt. PEC answers this call by providing tools that enable compliance while ensuring operational continuity.

Consider the healthcare industry, where patient data is both a valuable resource and a regulatory minefield. Traditional approaches to sharing and analysing such data—de-identification or anonymisation—often fall short, leaving gaps that can be exploited. PEC technologies, in contrast, allow collaborative research across entities like hospitals or pharmaceutical companies, unlocking insights without compromising privacy.

The rise of artificial intelligence and machine learning underscores PEC's importance. These models thrive on vast, diverse datasets, but accessing such data without breaching privacy is a challenge. PEC bridges this gap, enabling secure training of AI systems on distributed data sources.

The business benefits of PEC

For businesses, adopting PEC is a strategic investment. Companies that integrate PEC into their operations **gain a competitive edge** by establishing themselves as trustworthy custodians of customer data. Trust, in turn, fosters loyalty and can lead to increased market share.

Another important benefit is **risk mitigation**. Data breaches and non-compliance fines can cripple organisations, both financially and reputationally. PEC provides a robust framework to safeguard sensitive information, reducing the likelihood of such incidents.

Beyond compliance and risk reduction, PEC **opens avenues for innovation**. For example, it allows competitors to collaborate securely on shared challenges, such as financial fraud detection, without exposing proprietary data. This ability to unlock shared value while maintaining confidentiality, is a game-changer for companies in the finance, healthcare, or energy industries.





The technical landscape of PEC

To understand PEC's potential, we need to delve into its key technologies, (there are others, but we will focus on the key five).

Homomorphic encryption, a groundbreaking mathematical method that allows computations to be performed directly on encrypted data without the need for decryption. This ensures sensitive information remains secure throughout the process, making it particularly well-suited for scenarios such as cloud computing and financial analysis.

Secure multi-party computation (SMPC), which enables multiple parties to collaboratively compute a function without exposing their individual inputs. This approach is especially valuable for sensitive collaborations, such as when banks share fraud detection insights while maintaining the confidentiality of their proprietary data.

Differential privacy plays a significant role by introducing controlled noise into datasets, ensuring that individual data points cannot be identified while preserving the dataset's overall utility. This technique is widely employed in public data-sharing initiatives and in training artificial intelligence models to maintain privacy.

Secure enclaves provide a robust solution by isolating sensitive computations in protected environments. These are frequently utilised in cloud infrastructures to enhance security, offering a dependable layer of protection for critical operations.

Zero-knowledge proofs present a powerful cryptographic tool that allows one party to verify their knowledge of specific information to another without disclosing the information itself. This innovative approach is highly effective in systems like identity verification, ensuring both security and privacy.

Key considerations for businesses

Despite its promise, PEC is not without challenges. Implementing these technologies requires significant computational resources and expertise. Additionally, businesses must evaluate the trade-offs between security and performance.

Regulatory ambiguity is another hurdle. While PEC aligns with privacy laws, the lack of clear guidelines on its implementation can create uncertainty. Businesses must work closely with legal experts and policymakers to navigate these waters.

Understanding the limits of PEC is an absolute must. Not all data sharing problems can be solved with PEC, and businesses must discern between genuine solutions that will provide benefits and market hype.





What should businesses do today?

For organisations looking to leverage PEC, the journey begins with awareness and assessment. Here's a roadmap to get started:

1. Firstly, **evaluate your data practices**, thoroughly analyse the types of data your organisation handles, and pinpoint the areas where privacy concerns are most pressing. Once that is performed, you can identify the key opportunities for integrating PEC technologies.
2. Next, and not to be avoided, **invest in expertise**, a successful implementation of PEC relies on a strong technical foundation. Organisations should focus on developing in-house talent or collaborating with experts who specialise in PEC technologies to ensure a smooth transition and a successful outcome.
3. **Collaboration and piloting** are equally important. Engaging with industry peers or partnering with academic institutions to pilot PEC-based projects can provide valuable insights and help refine strategies before scaling up.
4. To ensure compliance, organisations must **monitor evolving regulations**, staying up-to-date with privacy laws and align PEC implementations accordingly. This not only avoids legal risks but also strengthens trust with stakeholders.
5. Lastly, fostering a culture of privacy is vital, which begins by **educating stakeholders**. Promoting awareness among employees, customers, and partners about the importance of privacy builds trust and paves the way for smoother adoption of PEC solutions.

Concrete applications of PEC

To illustrate PEC's transformative potential, here are five specific use cases:

- In **collaborative pharmaceutical research**, multiple companies leverage PEC to analyse vast patient datasets in their quest to identify groundbreaking drug development opportunities. By ensuring that individual patient records remain completely confidential, this approach not only accelerates innovation but also builds trust with patients and regulators. For pharmaceutical professionals, this means a faster and safer route to life-saving treatments without ethical or legal hurdles tied to data privacy.
- For **fraud detection in banking**, PEC technologies like secure multi-party computation (SMPC) enable financial institutions to share insights about suspicious transaction patterns. Without exposing customer data, banks can collectively identify fraudulent activities, bolstering the entire financial ecosystem's resilience. This approach directly addresses the banking industry's dual challenge of fighting fraud while adhering to strict privacy regulations.
- When it comes to **smart cities and IoT security**, differential privacy ensures that the massive volumes of data collected by urban sensors remain anonymous. Planners can analyse traffic patterns, energy usage, and other critical metrics to improve city efficiency while protecting residents' individual activities. For urban developers and IoT professionals, this balances technological advancement with the public's demand for privacy.
- In **federated learning within healthcare**, hospitals collaborate to train advanced AI models using encrypted patient data. This enables the creation of highly accurate diagnostic tools without centralising sensitive information. For healthcare providers, PEC solves the challenge of balancing cutting-edge AI development with the need to maintain stringent patient confidentiality standards.
- Finally, **cross-border data sharing** becomes a secure reality through PEC-powered secure enclaves. Government agencies can share intelligence about cyber threats, enabling coordinated international responses without risking national security. For public sector professionals, this fosters global cooperation while ensuring their nation's sensitive information remains protected.



So what to do next

PEC is more than just a technological breakthrough – it represents a paradigm shift in tackling data privacy and utility challenges. PEC enables organisations to address one of the digital age's most critical issues: using data responsibly, while unlocking new opportunities.

Zenitech's experts are key players in this transformation, assisting businesses across various industries in addressing their unique data challenges. Working closely with clients and industry specialists, Zenitech ensures tailored solutions that drive innovation, foster trust, and deliver measurable value. Embracing PEC isn't just a forward-looking strategy – it's an opportunity to shape the future of secure and ethical data usage today.

Reach out to our team to discuss how PEC can transform your data privacy strategy.




zenitech




Connect with us

 www.zenitech.co.uk

 info@zenitech.co.uk

 [linkedin.com/company/zenitechteam](https://www.linkedin.com/company/zenitechteam)

 [facebook.com/zenitechteam](https://www.facebook.com/zenitechteam)

 [instagram.com/zenitech](https://www.instagram.com/zenitech)