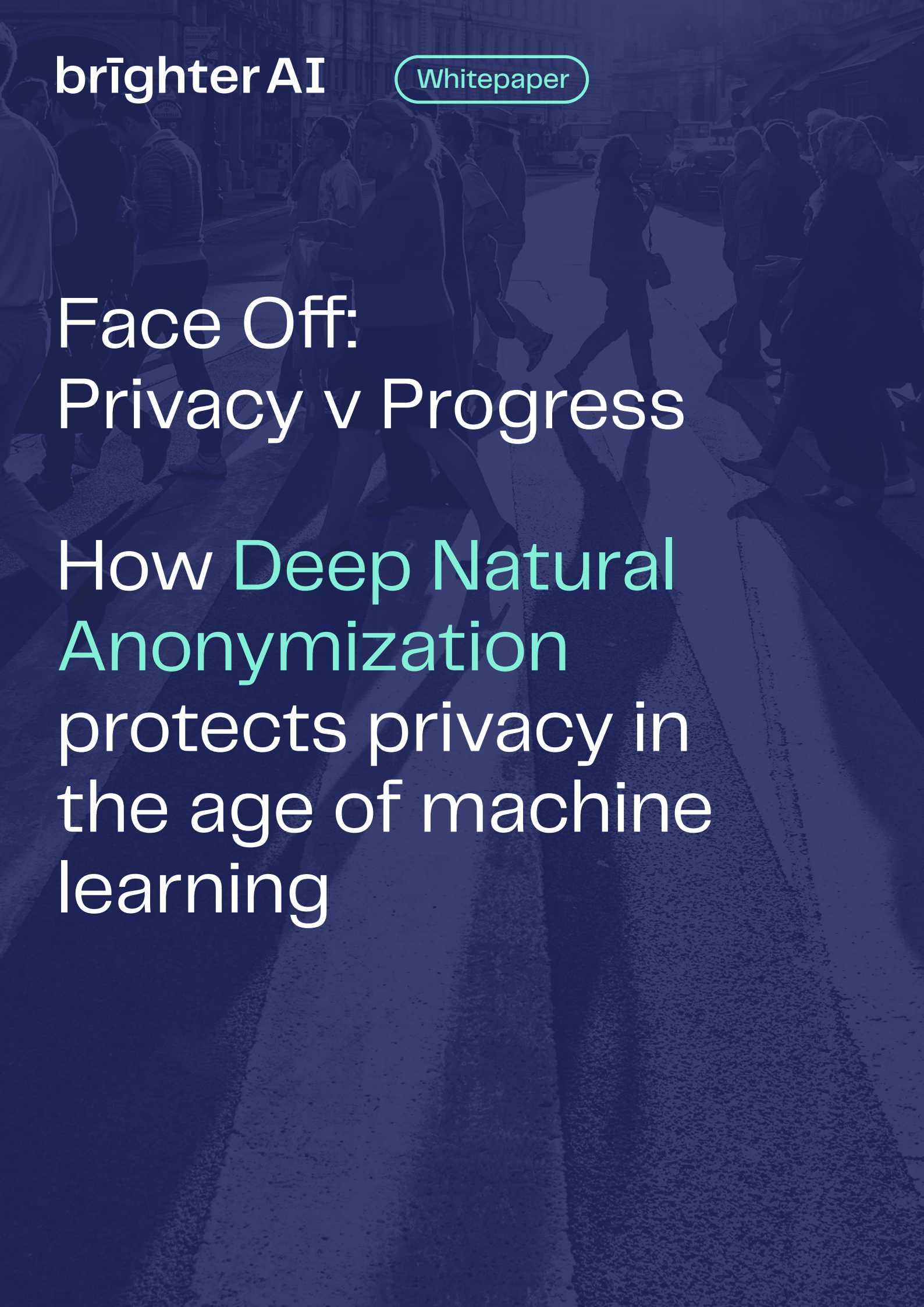
brighter AI

Whitepaper



Face Off: Privacy v Progress

How Deep Natural Anonymization protects privacy in the age of machine learning

Abstract

AI innovation, smart analytics, and machine learning are shaping the future. We see their impact in everything from autonomous vehicles and digital therapeutics to law enforcement and scientific research. Yet to work effectively and power innovation, these technologies require substantial amounts of high-quality image and video data.

At the same time, personal privacy is becoming more tightly controlled than ever by regulations such as CCPA in the US, PIPL in China, and, above all, GDPR in the EU. So how do organizations pursue innovation while remaining compliant with such exacting standards?

Anonymization techniques such as pixelation and black bars have long been the traditional response to this dilemma. However, they cannot preserve the accuracy and integrity of the original data. Since quality data represents the backbone of AI innovation and machine learning, the result is a trade-off between privacy and video analytics.

This report explains how Deep Natural Anonymization (DNAT), a generative AI-based technology, has changed the game. By preserving the quality of the original data while ensuring compliance to global standards, it eliminates the compromise between privacy and innovation.

> Predicting the future isn't magic, it's artificial intelligence.
>
> – Dave Waters, University of Oxford

1

The GDPR: A very private affair

The General Data Protection Regulation (GDPR) is not just a legal framework for protecting personal data. It represents one of the toughest privacy and security laws in the world.

The EU may have drafted and passed the regulation, yet it imposes obligations onto any organization, anywhere, that collects data relating to EU citizens.

That means that if you process the personal data of EU citizens or residents, or offer goods or services to them, the GDPR applies to you – even if you're not based in the EU.

The GDPR levies severe fines against any company that violates its standards – up to 20 million euros or 4% of global revenue, whichever is higher. The subjects of any breach also have the right to seek compensation for damages. At a time when ever more people are sharing their personal data with cloud-based services, the GDPR highlights the seriousness Europe now places on data privacy and security.

In an age where the power of facial recognition technology is becoming ever greater, so too does the responsibility for organizations to meet increasingly stringent privacy regulations.

The 7 principles of GDPR

1. Lawfulness, fairness, and transparency
Obtain the data on a lawful basis, fully inform the individual, and keep your promises.

2. Purpose limitation
Be specific and inform your clients about the purpose of the data collection.

3. Data minimization
Only collect the minimum amount of data required for the intended purposes.

4. Accuracy
Personal data must be accurate and where necessary kept up to date.

5. Storage limitations
Data must be kept in a form that allows data subjects to be identified for the minimum length of time possible.

6. Integrity and confidentiality
Protect data against unlawful processing or accidental loss, destruction, or damage.

7. Accountability
Record and prove compliance and be able to show the documents that prove this.

2

DNAT: driving innovation, ensuring compliance

The fast-growing capabilities of facial recognition technology are becoming an integral driver for innovation. At the same time, privacy regulations such as GDPR have become far more robust. This means that video data collection can pose a significant challenge to any organization that relies on such data to pursue progress – especially with conventional anonymization solutions like blurring or pixelation incapable of preserving the accuracy and integrity of the original data.

Have we reached the point where privacy regulations threaten to brake – or even block – innovation?

What is DNAT?

Deep Natural Anonymization is a unique privacy technology based on generative AI. It uses artificial replacements in video and images to protect individuals from being recognized: creating synthetic face overlays or replacing license plates with replicas.

At the same time, DNAT maintains the data quality required for machine learning. This allows organizations to safely use videos and images to power AI and analytics, yet without the threat of receiving heavy fines, losing customer trust, and damaging reputations.

Why use Deep Natural Anonymization (DNAT)?

It's safe: re-identification by facial recognition technology is impossible, with synthetic faces randomly generated and non-reversible.

It's accurate: age, gender, race, emotions, facing direction, and intention are retained for analysis and AI development.

It's compliant: EuroPriSe certification for privacy-compliant IT products.

> This anonymization technique is much more valuable than simply blurring faces and license plates. Facial features and physical attributes can still be recognized, and data can be used to train machine learning models. DNAT combines technical innovation with effective protection of personal privacy, distinguishing it from other redaction techniques. Importantly, this approach ensures that video recordings remain compliant with the strict data protection guidelines stipulated by GDPR and other regulations.
>
> – Philipp Wende, Senior Consultant Automotive & Innovation Program Lead, DXC

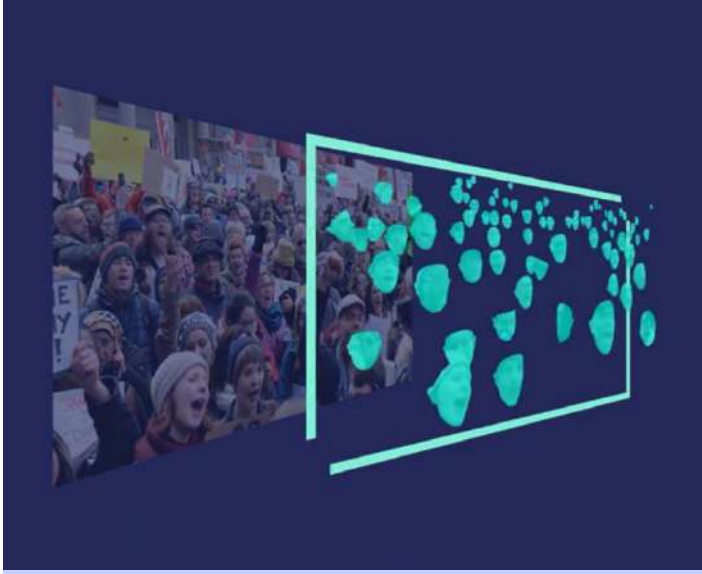
3

How does DNAT resolve the progress/privacy dilemma?

DNAT uses AI to automatically detect faces and other identifiable elements such as license plates in the original images and videos. The technology then randomly generates artificial replacements that reflect the original attributes.

For example, it is often important to preserve facial attributes such as gender, emotions, intent or age for further analytics. DNAT retains any information that does not contain sensitive personal data without modification. In doing so, it effectively removes the compromise between anonymizing data and retaining the original quality.

The technology then applies these non-reversible overlays to the original, ensuring that re-identification by facial recognition technology is impossible.



How does DNAT work?

1. DNAT automatically detects faces in the original image.

2. An artificial overlay is generated for each face.

3. These non-reversible overlays replace the original face.

> This technology makes data collection in public compliant according to privacy regulations worldwide, such as GDPR in Europe, CSL in China and the upcoming CCPA in the US.
>
> – The Washington Post, March 21st, 2019

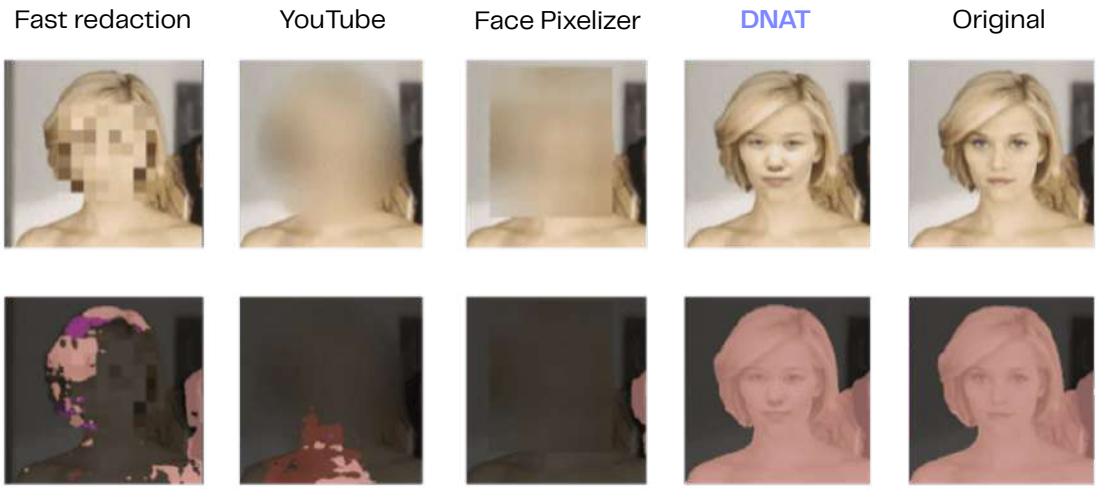
Method	MIoU (%)
Fast redaction	65.7
YouTube	74.9
Face Pixelizer	88.1
DNAT	**98.5**

MIoU refers to “mean Intersection over Union”. The higher the number, the less impact the anonymization method has on the unmodified image.

DNAT v Conventional anonymization

Conventional anonymization solutions, such as blurring or black bars, are not compatible with analytics and machine learning and compromise data quality.

In contrast, DNAT keeps data natural but compliant, yet also retains attributes such as age and gender to preserve semantic segmentation.



Reese Witherspoon DeepLabv3 + segmentation. First row shows the input images to the model and the second row the segmentation map overlayed onto the input image.

4

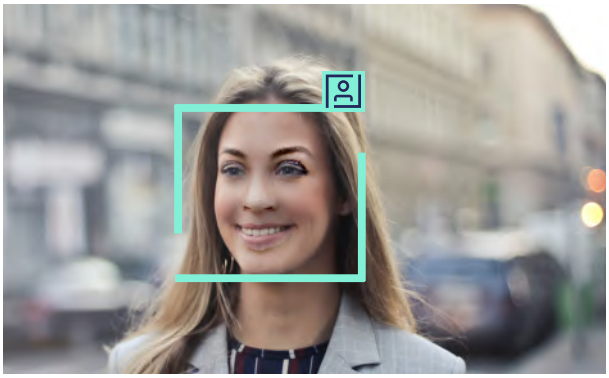
Meet brighter AI

brighter AI's DNAT is the only certified value-preserving video redaction software to assure GDPR compliance. In doing so, we end the trade-off between privacy and video analytics.

Our highly advanced anonymization software protects personally identifiable information (PII) in image and video data. It guarantees that your data complies with privacy regulations like GDPR, CCPA, APPI and PIPL. At the same time, our software preserves the data quality of the original image to drive AI innovation and machine learning.

Original

Anonymized with DNAT



Identities protected
Natural appearance
Applicable for analytics and machine learning

> brighter AI has solved a fundamental problem of using and storing image and video data in compliance with data protection regulations.
>
> – Handelsblatt, Nov. 23rd, 2019

brighter AI uses deep learning to recognize objects: artificial neural networks trained on large data sets including a range of resolutions and perspectives. This offers a higher degree of accuracy and robustness compared to conventional approaches. If you find this interesting, check out our report on the accuracy of machine learning models trained on anonymized data.

Approved by privacy professionals and research scientists, brighter AI anonymization software seamlessly integrates into any platform from edge to on-prem to cloud. And it is backed up by cloud compliance & data protection warranties, full support, and zero maintenance costs.

> DNAT automatically detects a personal identifier such as a face and generates a synthetic replacement, protecting identities while keeping necessary information for analytics or machine learning. brighter AI provides the world's most advanced image and video redaction technology
>
> – Marian Gläser, CEO & co-founder

What industries are using DNAT the most?

Privacy v Progress #1

brighter AI for automotive

brighter AI is designed for automotive data collection in compliance with the latest privacy standards. Supporting both current development projects as well as future vehicle fleet data collection, the software is ideal for training machine learning models such as autonomous driving without compromising data quality.

brighter AI's solution was easily integrated and the natural anonymization was what we needed for improvement of line & detection validation strategy.

– Vaclav Schiybel, System validation platform manager, Valeo.

Privacy v Progress #2

brighter AI for healthcare

In sensitive medical video and image data, it is critical to anonymize patients and staff. brighter AI provides the leading automatic anonymization software for healthcare use cases at scale. Applications range from user experience and machine testing to digital therapeutics, education and research, and patient tracking.

We decided to use the service of brighter AI, because the functionality to anonymize persons works very well. We were particularly surprised by the accuracy of the recognition method. The API was well documented and could be quickly integrated into a cloud solution.

– Jens Dürasch managing director, OnREX GmbH

Privacy v Progress #3

brighter AI for public sector

brighter AI supports the privacy-compliant use of intelligent video analytics and storage of image and video data. This allows data to be legally processed for video-based analysis or the training of machine learning models within both the public and private sector. Check out how BVG used our solution to include compliant e-learning videos in tram driver training & improved operational efficiency.

brighter AI in action
Trusted by Deutsche Bahn
Privacy compliant intelligent videos analytics at Berlin's main train station.

We helped Deutsche Bahn, the largest transportation provider in Germany, to use existing camera infrastructure for intelligent video analytics in trains and stations – as well as the development of autonomous trains. This allows the organization to effortlessly meet data protection goals and accelerate digitalization in a trustworthy and socially responsible manner.

Privacy v Progress #4

brighter AI for research

brighter AI supports data collection, sharing and storage for universities and companies engaged in computer vision, machine learning and deep learning research. Classic and AI-compatible redaction tools provide the highest detection accuracy. Applications range from scientific and behavioral research to publications and collaborative databases.

Together with our university partners and Facebook AI Research, we decided to use the brighter AI software to anonymize data sets within our computer vision research. We appreciate the accuracy of brighter AI's anonymization solutions, the possibility of a simple on-premise set up, as well as the great support by the brighter AI team.

– Bernard Ghanem, Associate Professor, King Abdullah University of Science and Technology.

Conclusion: The new face of anonymization

Data has become an integral driver of innovation. At the same time, increasing robust and expansive privacy laws place tight restrictions on how this data can be used.

Conventional anonymization technology lacks the capability to preserve data quality, threatening to slow down or even stop progress altogether. As the next generation of anonymization, DNAT resolves this face-off.

After all, innovation is essential for growth. According to Booz & Co, innovative organizations boost revenues by 11%. Yet bitcom.org estimates that 90% of companies have had to put innovative projects on hold because of data protection requirements. And three quarters say that the concrete requirements of the GDPR have directly resulted in the failure of innovation projects.

By retaining the quality of the original data in a way that complies with all global privacy regulations, DNAT resolves the privacy v progress dilemma. In doing so, it frees organizations to drive innovation safely and responsibly.

The consequences of not using DNAT

1. Continued use of compromised data for machine learning leads to a negative impact on products, poor CX, and a loss of competitiveness and revenue.

2. Stop using data altogether, resulting in blocked or failed innovation projects.

3. Use unmodified original data without complying to privacy standards, risking significant fines and negative publicity.

The fines handed out for breaches of data law totaled €555M in 2022 (until October).

Source: enforcementtracker.com

Want to know more?

Contact us

Would you like to see brighter AI in action? Or discover how we can help you power your AI innovation, smart analytics, and machine learning while remaining compliant with global privacy standards? Just get in touch and we'll be happy to help.

Brighter AI Technologies GmbH, Registry Court: Berlin Charlottenburg hrb 188087, Managing directors: Marian Gläser and Tobias Stelzer; hello@brighter.ai