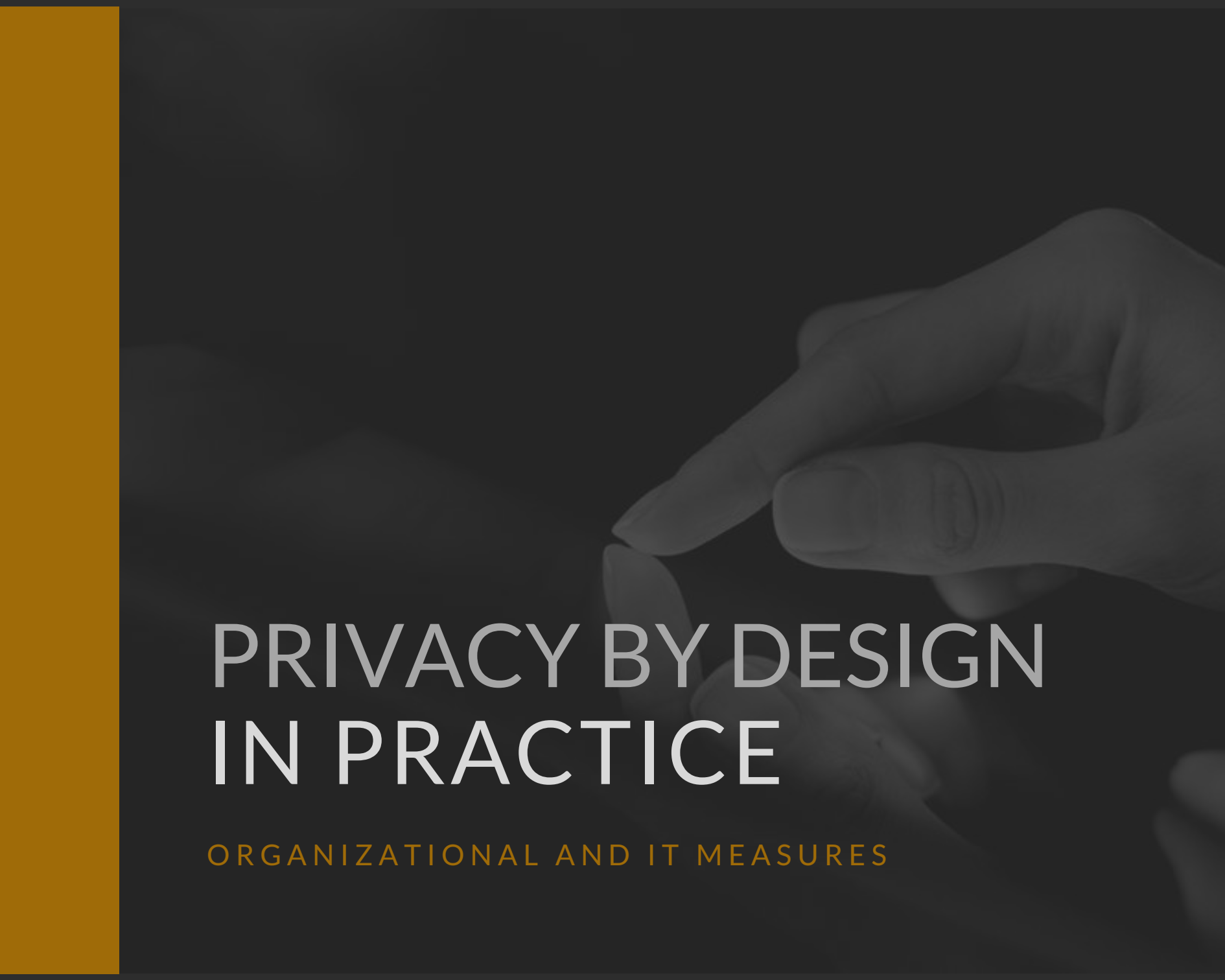


PRIVACY BY DESIGN IN PRACTICE

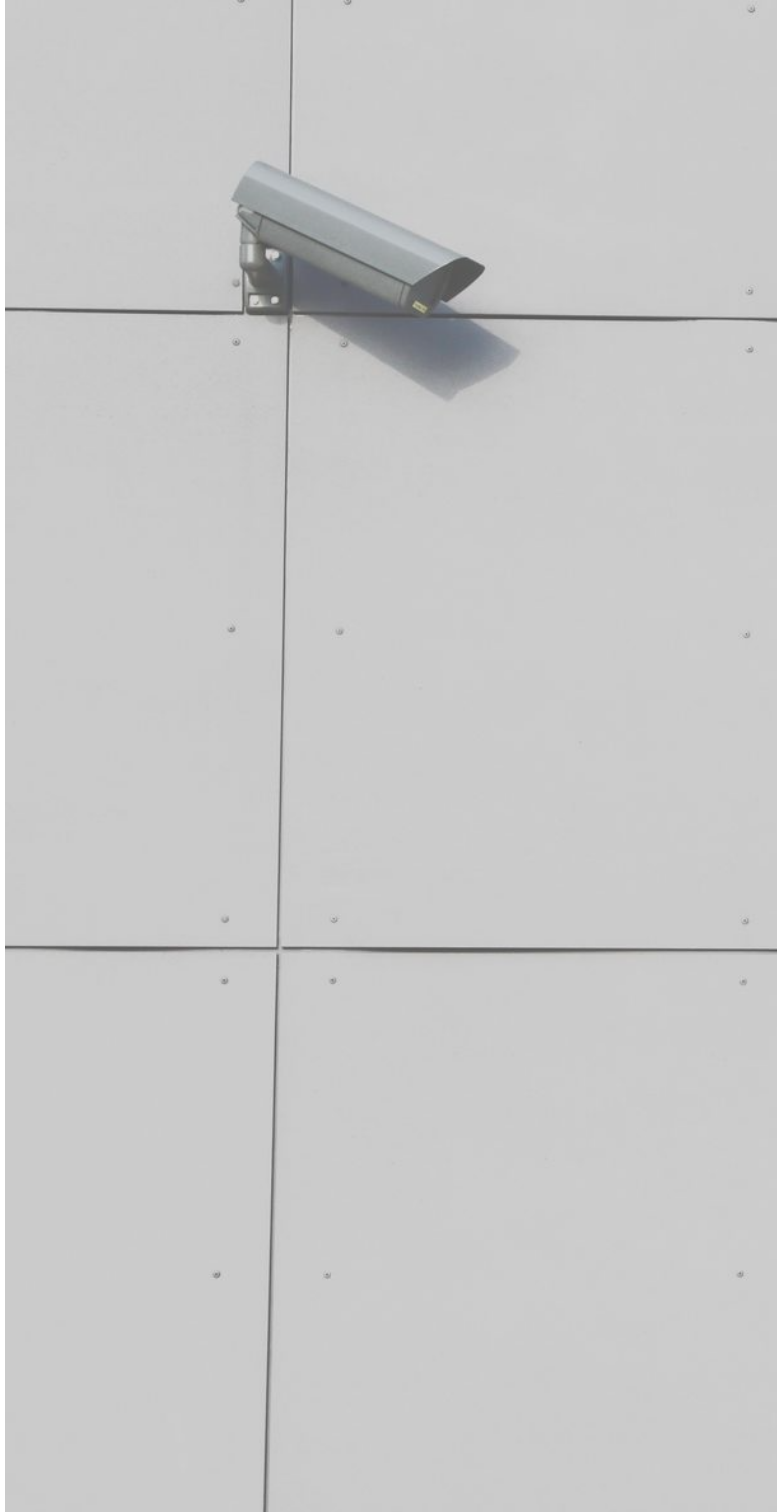
ORGANIZATIONAL AND IT MEASURES

GDPR
And Data Privacy

The past year saw the acceleration of two already important information **security trends**:

- the ever-increasing threat of **data breaches**
- a rising **consumer and regulatory oversight** on corporate data processing

Indeed, the year was not a good one for privacy – high profile data breaches range from the Marriott Hotels (**500** million people), through marketing firm's Exactis (**340** million), all the way into India's national identification system (**1.1** billion people).



It is little surprise that on both sides of the ocean, **regulators and advocacy groups are intensifying their scrutiny.**

In the EU the most visible initiative was an ambitious General Data Protection Regulation with strict requirements on processing. This is secured by fines of up to 4% of global revenues of wrongdoers.

In the US we have observed a number of high-profile lawsuits such as the consolidated class action against Facebook. This comes against the backdrop of more activity on the part of the **Federal Trade Commission.**

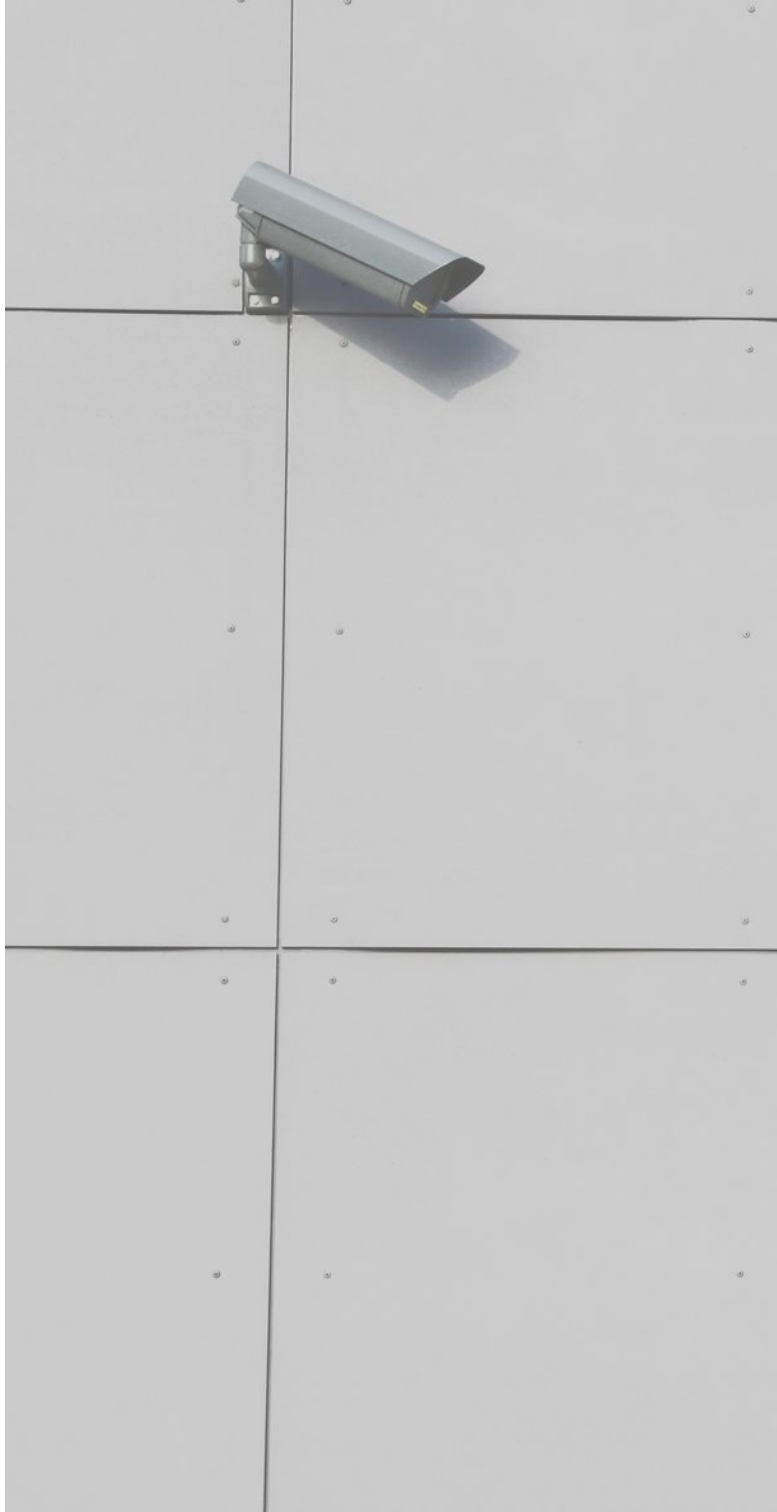
In the EU and the US regulators and advocacy groups are intensifying their scrutiny.

Privacy by Design

Data breaches are bad for both business and consumers, leading to ruined reputations, decreased trust, increased churn, and direct operational and legal expenses.

On the other hand, preventing data breaches remains a challenge. Thus, the requirements on system development increase by mandating the baking-in of privacy into the Software Development Life Cycle.

This is the new paradigm of **Privacy by Design,** also enshrined in **Article 25** of the GDPR. Initially conceived by Ontario's Information Commissioner Dr. A. Cavoukian, it consists of seven broad overarching principles:



PRIVACY BY DESIGN: 7 PRINCIPLES

1. **Proactive** not reactive | **Preventative** not remedial
2. Privacy as the **default** setting
3. Privacy embedded into **design**
4. **Full functionality:** positive-sum, not zero-sum
5. **End-to-end security:** full lifecycle protection
6. **Visibility** and **transparency:** keep it open
7. **Respect** for **user privacy:** keep it user-centric

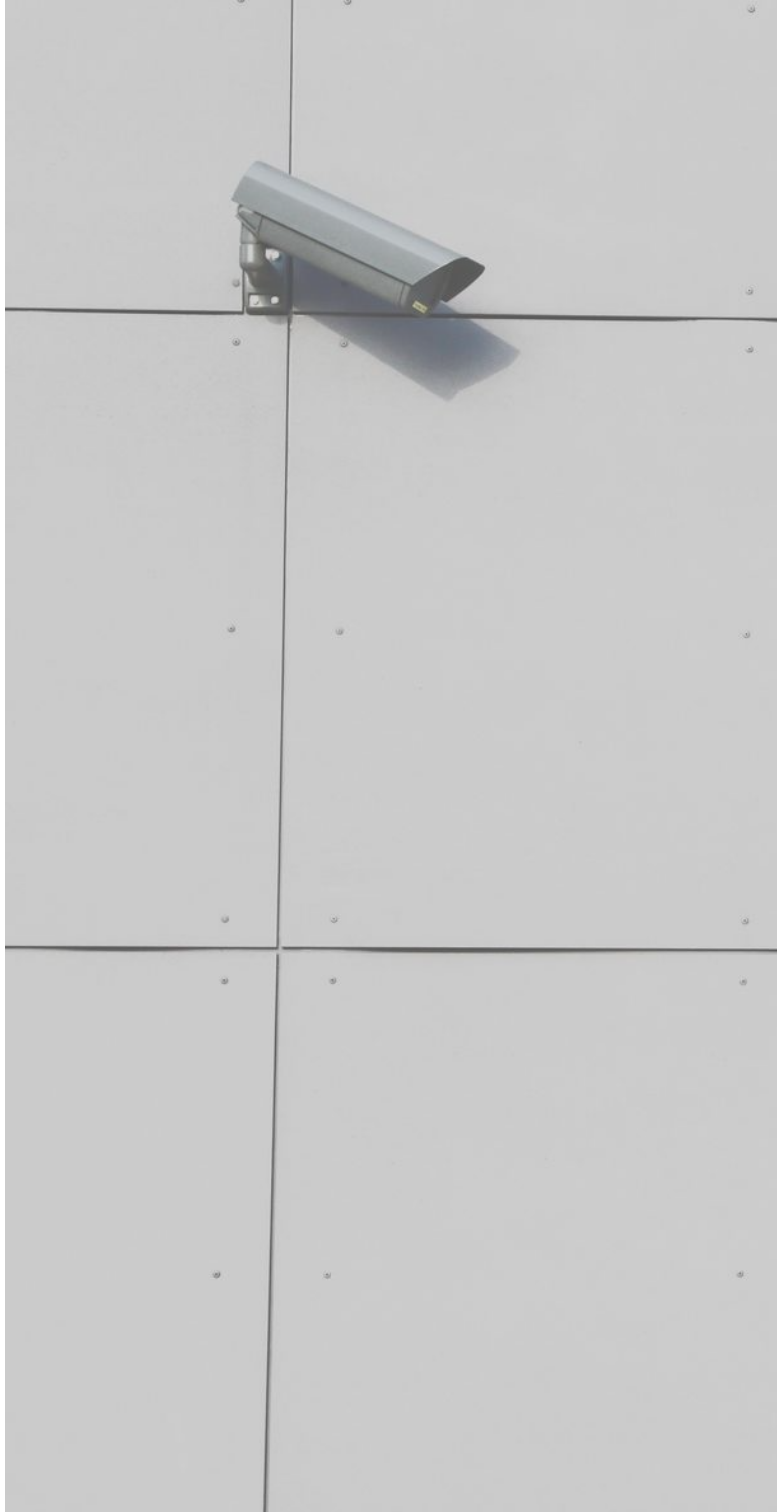
Organizational and IT Measures

How do those lofty principles fit in practice?

They require a convergence of organizational practices and technological measures that provide for a high level of data protection.

The organizational side is the more familiar one: a combination between policies, processes, and standard operating procedures is must. This is then meshed together with a strong management push and extensive training towards a privacy-friendly culture.

While this is more easily said than done, implementation is still within reach for (almost) all organizations.



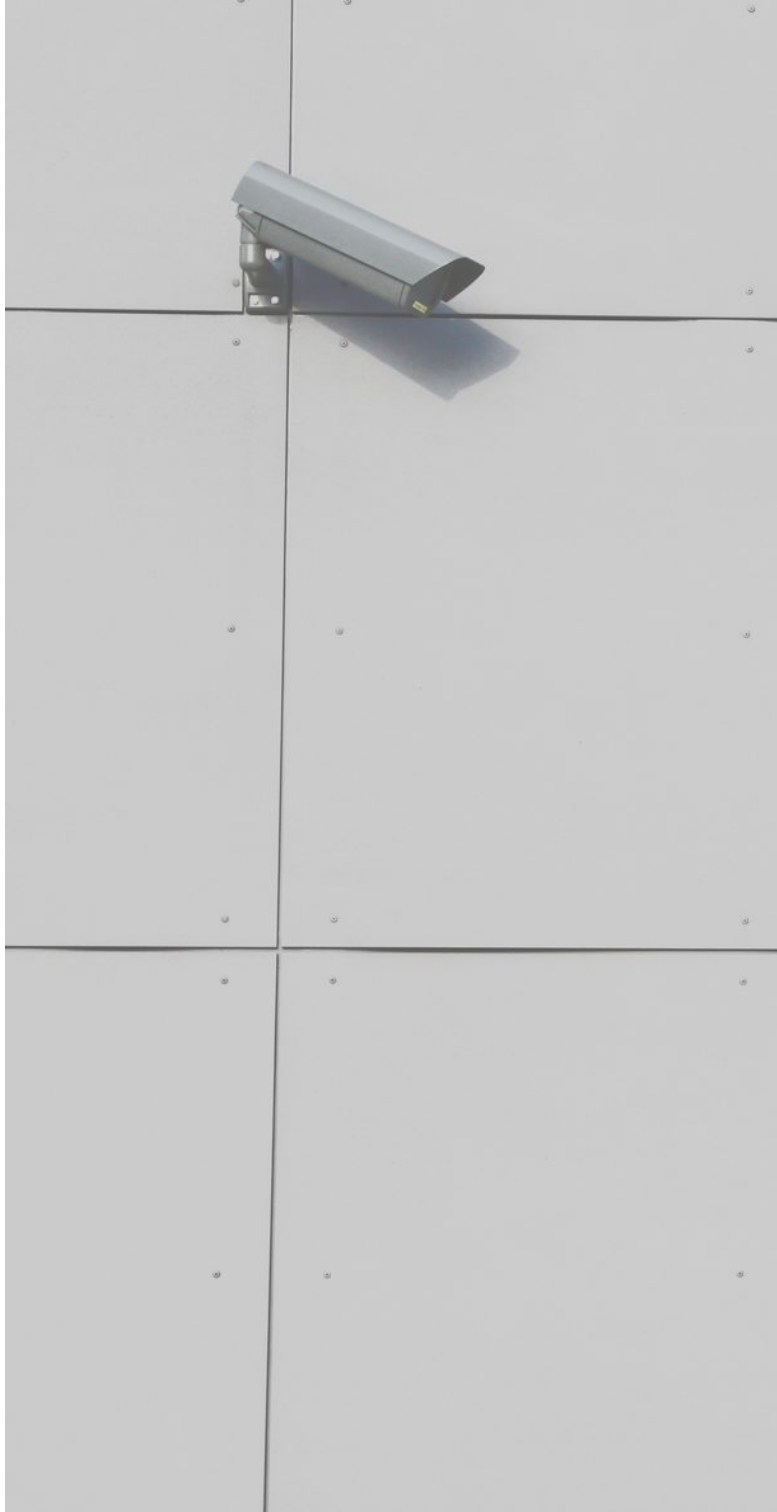
On the technological side, things are more complicated.

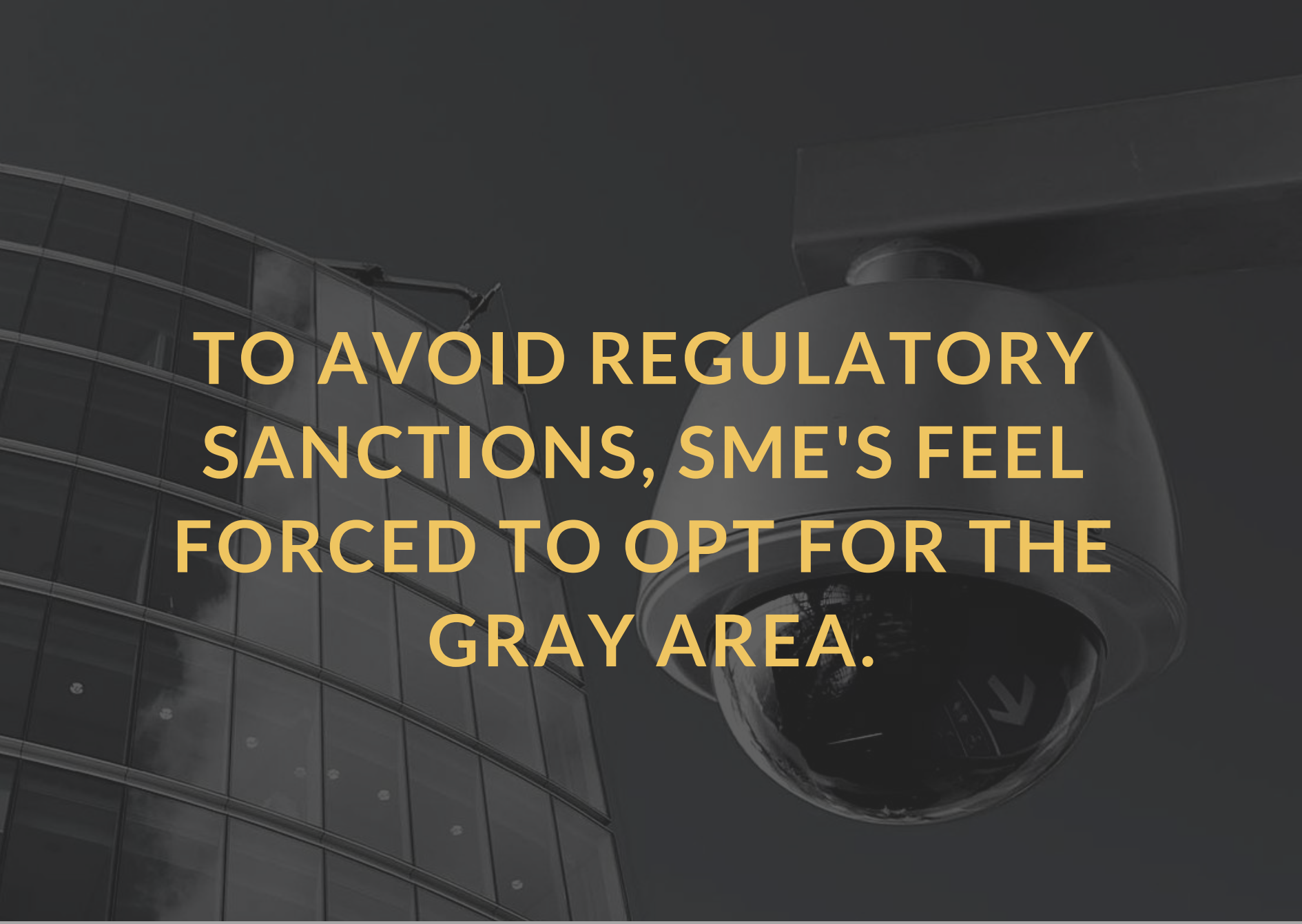
While privacy-enhancing technologies (PETs) have proliferated, they remain merely pieces of the privacy puzzle.

Developers and security officers do have an understanding that a combination of secure multifactor authentication, strict access controls, data encryption and tamper-free logging are important components of the security architecture.

Companies have to **piece all those components together.**

The context and the risk assessment will call for additional ones, and then the entire solution is to be rolled out and continuously supported. Given the **v**ast amount of human and financial resources needed, this is a formidable challeng**e** for even large organizations, let alone the **medium and small business.**




TO AVOID REGULATORY SANCTIONS, SME'S FEEL FORCED TO OPT FOR THE GRAY AREA.

Real-life Implementation

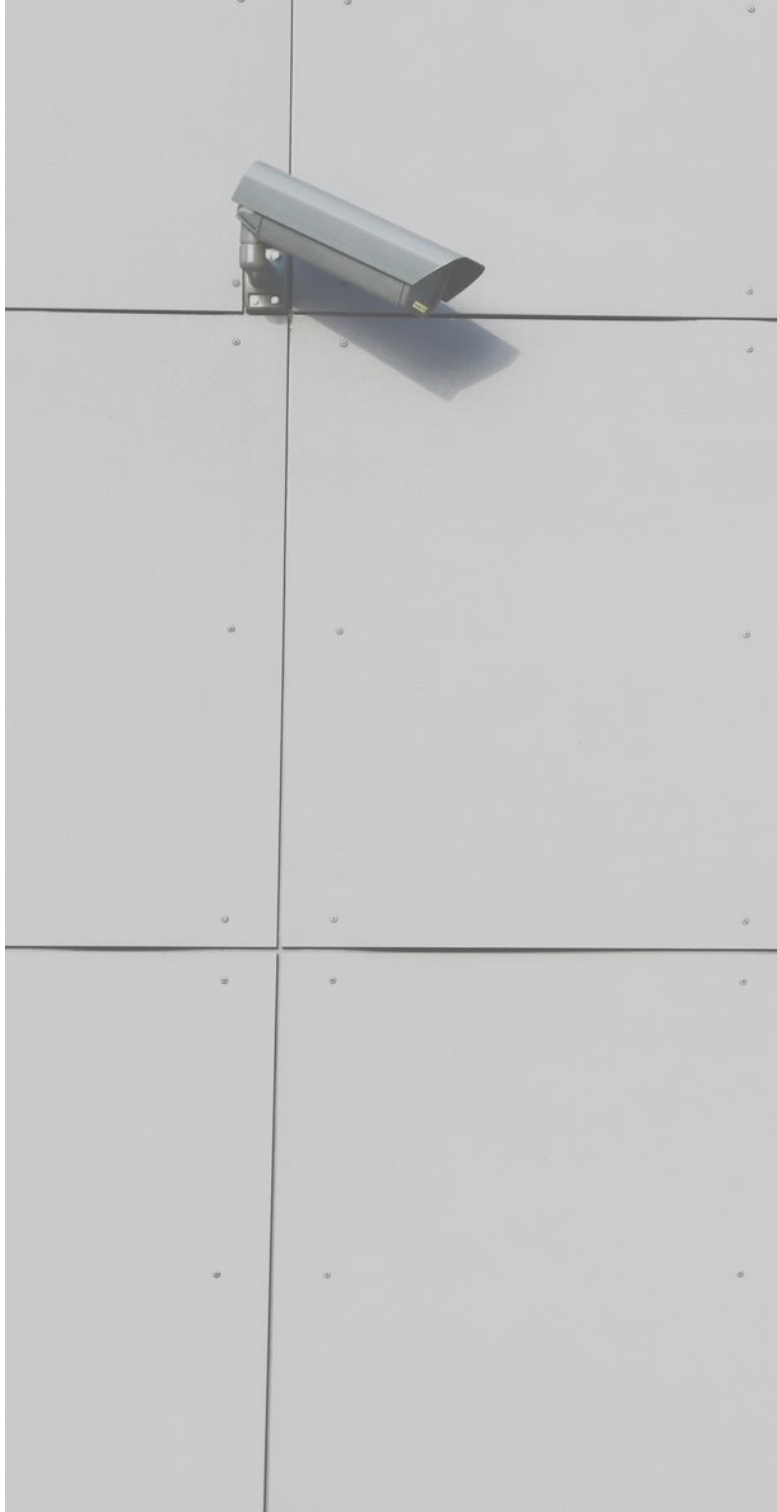
What does it cost to become compliant?

Some businesses opt for the gray area where they implement subpar protection in the hopes that regulators, activist consumer groups or competitors will not catch up on this.

This needlessly exposes them to business risk that may be massive in scope.

A potential solution to this problem is to **leverage a cost-efficient proprietary solution** that takes care of most, if not all, of the **compliance needs.**

External vendors leverage economies of scale and scope and can provide both cutting-edge technology and advanced legal and organizational support.



SentinelDB

The 'Privacy by Design' database

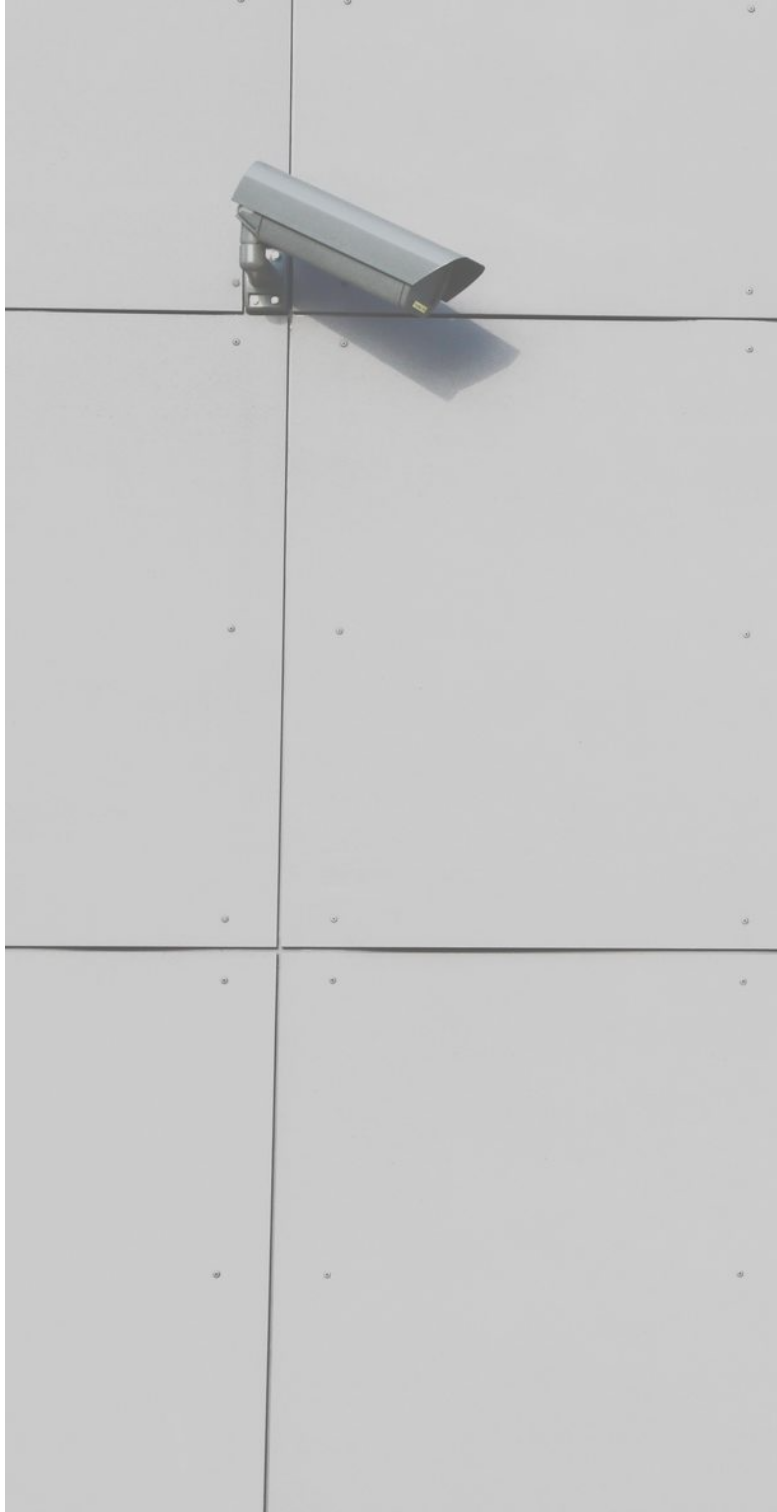
Our product SentinelDB is a **fully compliant** and extremely **secure database** on the cloud that effectively prevents data breaches.

We are able to offer **multiple levels of encryption**, AI-driven **anomaly detection**, and **blockchain-enabled logging capabilities,** thus bringing privacy protection to the next level.

Irrespective of the solution, however, businesses will need to be conscious of privacy protection if they are to continue using and generating profit from a crucial asset – personal data.

Try our secure database today and see how it keeps every record securely:

https://logsentinel.com/sentineldb/



What We Offer

PROTECTION OF ANY TYPE OF PII

We offer a 'Privacy by Design' secure database. We encrypt every record individually, using a secure key hierarchy making data breach events practically impossible.

KEEPING UNMODIFIABLE LOGS OF ACTIVITY

Most of the data breach attempts are initiated by insiders. Very often insiders man age to cover their traces making it impossible to track back who has breached the d ata. With SentinelTrails, your activity logs will be kept safe on blockchain , so that no one would be able to access your data without any evidence

FRAUD AND ANOMALY ACTIVITY DETECTION

Thanks to the advanced technology used for developing SentinelTrails, you can rec eive real time notification if anomal activity is detected - e.g. access to PII outside of work hours

EASY INTEGRATION. ZERO MAINTENANCE.

Minimum efforts are required from your side. Our expert team will adapt our servic es to the exceptional requirements of your organization, so that you can focus on w hat's actually important - saving lives.

INFORMATION SECURITY, DATA PROTECTION & COMPLIANCE

WWW.LOGSENTINEL.COM