# Privacy & Security Sheet

Proactive Safety Powered by AI

# Security: How we do it

**We take your data and trust seriously and have built our processes and products to ensure the highest grades of security and privacy.**

We take a privacy-first approach to everything we build. Our platform is built upon the latest privacy and security published research frameworks with state-of-the-art security and privacy tools. This enables us to keep customer data secure and preserve its privacy throughout every part of our system. This allows our customer complete ownership over your data in our system, allowing you to manage access levels, access, modify and delete data upon request.

**We manage your data transparently by ensuring you have complete control and ownership of it.**

**Secure System Architecture**

Pro AI is built using Edge Computing which maximizes the efficiency of cloud platforms with the security of on-site deployments. By installing the Vision Edge Device onsite, all your data, such as video streams, are processed **within your network** whilst only event data is encrypted and sent to the cloud.

**ISO27001 Certified**

We take your data and trust seriously and have worked hard to adhere to the highest possible standard that the **ISO 27001** certification presents. We take your d**ata and trust seriously** and have worked hard to adhere to the highest standard

We have established stringent processes to ensure that the fundamental principles of Privacy by Design (PbD) are implemented across the entire AI platform.

# 7 Protex AI Data Privacy Principles

## Privacy by Design (PbD):

1. **Proactive not Reactive, Proactive not Remedial.** Privacy risks should be anticipated. PbD is a before-the-fact design measure to identify risks before they occur.

2. **Privacy as Default.** Setting for all your organization, your workers, and users of the platform.

3. **Proactive Embedded into Design.** Privacy shouldn't be an add on, it should be integral to the system design.

4. **Full Functionality- Positive Impact.** The implementation of privacy should not result in any unnecessary trade-offs with other system components

5. **End-to-End Security – Full Lifecycle Protection.** Strong Security measures are essential to ensure secure retention of data and safe destruction thereafter.

6. **Visibility and Transparency – Keep it Open.** All stakeholders of the system should be made aware of the privacy practices that are in place Respect for User

7. **Privacy – Keep it User-Centric.** The users of the system are core to and privacy-related decision

Ciarán O'Mara

# Person De-identification

## Managing the collective

**We don't compromise when it comes to ensuring the preservation of organizational and individualistic privacy (of your workers), it's as simple as that.**

We understand that privacy and security are a top priority for all our customers and as such, we have designed our system to manage the collective, instead of the individual. The AI system acts as an extra pair of eyes watching your CCTV feeds. The system only sees what it needs to, identifying nothing more (in terms of privacy) than a security guard would while identifying everything (in terms of safety) that your best EHS employee would.

**Using the power of the edge and on-prem processing we have implemented several de-identification measures**

- ☑ No Facial Recognition used
- ☑ Facial blurring
- ☑ Leveraging Metadata
- ☑ Facility-based insights instead of individually based
- ☑ Enable video masking, blurring, and privacy-preserving filters at the edge

This approach to the countering concepts of privacy, security, and safety empowers you to manage the collective, rather than the individual. Using the Safety Scores and Event Timelines, you can gain a greater understanding of the facility compliance and risk profiles.