Privacy by Design & Our Commitment to Data Protection

“Aura Vision's insights and analytics are anonymised data, do not constitute personal data under the EU GDPR and UK GDPR, and are created in line with regulatory guidance.”

— Mishcon de Reya, December 2025

Version history

Date	Version	Description	Owner
14 / 12 / 2021	v1.0	Initial version	Daniel Martinho-Corbishley
15 / 12 / 2022	v1.1	Taylor Vinters review	Daniel Martinho-Corbishley
17 / 12 / 2022	v1.2	Public release	Daniel Martinho-Corbishley
07 / 02 / 2023	v1.3	Version history added	Daniel Martinho-Corbishley
09 / 12 / 2025	V1.4	Mishcon de Reya review	
11 / 12 / 2025	v1.5	Public release	Daniel Martinho-Corbishley

Introduction

This White Paper sets out how Aura Vision services work to generate secure and anonymous analytics for end-users and how we have built our AI using a privacy-by-design approach to comply with the laws detailed below ("What laws apply?").

We also set out the data flow outline showing how data is processed from its initial collection via security cameras, right the way through to the creation of anonymous analytics made available on our cloud platform.

This White Paper is for anyone assessing the use of Aura Vision as an in-store analytics solution - from legal counsel to end-users. This document aims to help you systematically analyse, identify and minimise the data protection risks of using Aura Vision and helps you demonstrate compliance with your data protection obligations.

This White Paper is not meant to constitute legal advice or a contractual commitment. Instead, our aim is to expand and elaborate on what we do to comply with our obligations under data protection laws, so that our customers can make a better informed purchasing decision.

Mishcon de Reya LLP (Mishcon) have worked with Aura Vision to ensure Aura Vision are compliant with applicable UK data protection legislation and the EU GDPR.

Mishcon have not carried out a detailed assessment of Aura Vision's compliance with the EU AI Act, however Mishcon's provisional view is that Aura Vision's AI system will be limited risk, possibly even minimal risk under the EU AI Act (the 2 lowest of the 4 risk levels), meaning Aura Vision's obligation is to provide appropriate transparency information in their privacy notices (to the extent personal data is processed) and to ensure their team are aware of the risks and their obligations when using AI.

Contents

Feedback

We hope this clarifies how the Aura Vision AI works, but also what that means from a data protection regulatory position. If you think we have missed anything or there's anything further you'd like to know, please do let us know by reaching out to hello@auravision.ai.

What is Aura Vision?

Aura Vision is an AI solution helping brick-and-mortar retailers, shopping malls and commercial sites to drive sales and productivity in their physical locations, by better understanding their customers and day-to-day operations.

Using the latest advancements in computer vision, Aura Vision uses existing security camera infrastructure (CCTV) to anonymously count customer entries to each store, their demographics and movement, and staffing operations throughout each location.

Using existing security cameras means our solution is much more cost-effective and scalable, as it doesn't require significant and expensive sensor hardware to be installed.

This paper focuses on the legal principles associated with our technology, rather than how it works in detail. More detail in connection with how our technology works is available here.

What laws apply?

The principal legislation we comply with is listed below:

- The EU's General Data Protection Regulation (EU GDPR)
- The EU's Privacy and Electronic Communications Directive, and UK Regulations
- The UK's implementation of the General Data Protection Regulation following Brexit (UK GDPR)
- The UK's Data Protection Act 2018
- The EU Artificial Intelligence Act 2024
- California Consumer Privacy Act 2020

We take our obligations seriously regarding data protection legislation and have registered with the Information Commissioner's Office. You can find details of this registration here.

Data processing overview

Aura Vision supplies a small on-premise device (APU) that is plug & play connected to each store's security camera (CCTV) system. APU devices use Aura Vision's world-class AI algorithms to convert live video streams from security cameras into accurate and anonymous count,

movement and demographic analytics in real-time. These anonymous analytics are then made accessible to end-users via the Aura Analytics web platform (AAP).

During normal operation, all video is processed on-premise 'at-the-edge' and only anonymous, aggregated analytics are transferred over the internet to the Aura Analytics web platform (AAP) hosted on the AWS cloud in the EEA.

As video is processed on-premise, it never leaves the recording site and isn't streamed over the internet. This significantly minimises internet bandwidth requirements, which means Aura Vision can be deployed in locations with hundreds of cameras. As much processing as possible is completed on-premise, to follow privacy by design principles. This also helps mitigate security and privacy issues associated with transferring high volumes of video footage.

We have in place a number of technical and organisational measures to ensure the security of our processes, these can be found here.

AI model training

During initial setup, Aura Vision's team of Computer Vision experts will audit and fine-tune the AI models to improve the accuracy of people counts, age and gender demographics and train the algorithms to segment customers and staff based on uniform and clothing visual cues.

To facilitate this process, a small selection of face-blurred 'snapshot images' are transferred to our Aura Model Training (AMT) service hosted on the AWS cloud in the EEA, during the first week of the service. Snapshot images are not classed as personal data as individuals cannot be identified from them and the time and locations of images are not stored. The blurring process is non-reversible so the original images cannot be recreated from the blurred copies. Snapshot images are stored for a maximum period of two weeks. The AMT service is only accessible by Aura Vision's team of Computer Vision experts who all adhere to Aura Vision's code of conduct, IP protection, IT security and data protection compliance procedures.

Aura Vision have taken steps to ensure a sufficient level of AI literacy for staff, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, according with the EU AI Act.

No video storage

Aura Vision never stores or recalls historic video footage from surveillance systems. This functionality is left to the existing security camera system to facilitate security and surveillance use-cases.

No software integration

Aura Vision also doesn’t alter or interfere with the operation of the existing security camera system, and doesn’t require any installation of additional software on the existing security camera system. Instead, Aura Vision’s APU devices connect to the camera system as if they were another camera, enabling a straightforward and security risk-free plug & play setup.

Privacy-by-design

Since its inception in the UK in 2017, Aura Vision has been built following privacy-by-design principles, adhering to the requirements of the data protection legislation and information security standards.

The technology doesn’t use facial recognition, ensuring individual faces are never stored or identified. Faces in video footage are also blurred automatically to further protect individual identities. Video footage is processed in real-time and instantly discarded such that no personal data is stored at any point.

100% Anonymous

Aura Vision never stores or transmits personal data from video cameras. This allows Aura Vision to be deployed in public spaces and retail stores in any country, as it complies with the UK's stringent personal data regulations.

Video is turned into anonymous count analytics by APUs on-premises and discarded immediately during normal operation. Only anonymous count analytics are then transferred to Aura Vision's cloud Insight Platform.

No customer sign-up

Because Aura Vision doesn't store or transmit personal data there is no need for customers or employees to sign-up to additional T&Cs or sign-in to a WiFi landing page.

Instead, a small sign notifying customers about the purpose of collecting analytics at the entrance of the location is usually sufficient to comply with the data protection legislation.

In short, we don't process a great deal of personal data at all, check out our privacy policy to find out more.

Face blurring

Aura Vision incorporates face-blurring technology at source, to remove any identifiable information or meta data such as time and location, as soon as the video is processed. This ensures any images shared with our team of Computer Vision experts for training and auditing have already been anonymised and cleaned of any personal data.

Edge processing

Our APUs process all video on-device and only transfer anonymous count analytics to our cloud Insight Platform. This not only minimises upload bandwidth, but also prevents the transfer of any personal data during normal operation.

No sensitive data

Aura Vision never collects sensitive types of personal data, classed as Special Categories of Personal Data under UK GDPR.

Clean heatmaps

Heatmaps and camera thumbnails viewable on the Insight Platform dashboard are 'pre-cleaned' to remove any visible person before being uploaded.

Even more information on our approach to data privacy and IT security can be found at https://www.auravision.ai/security.

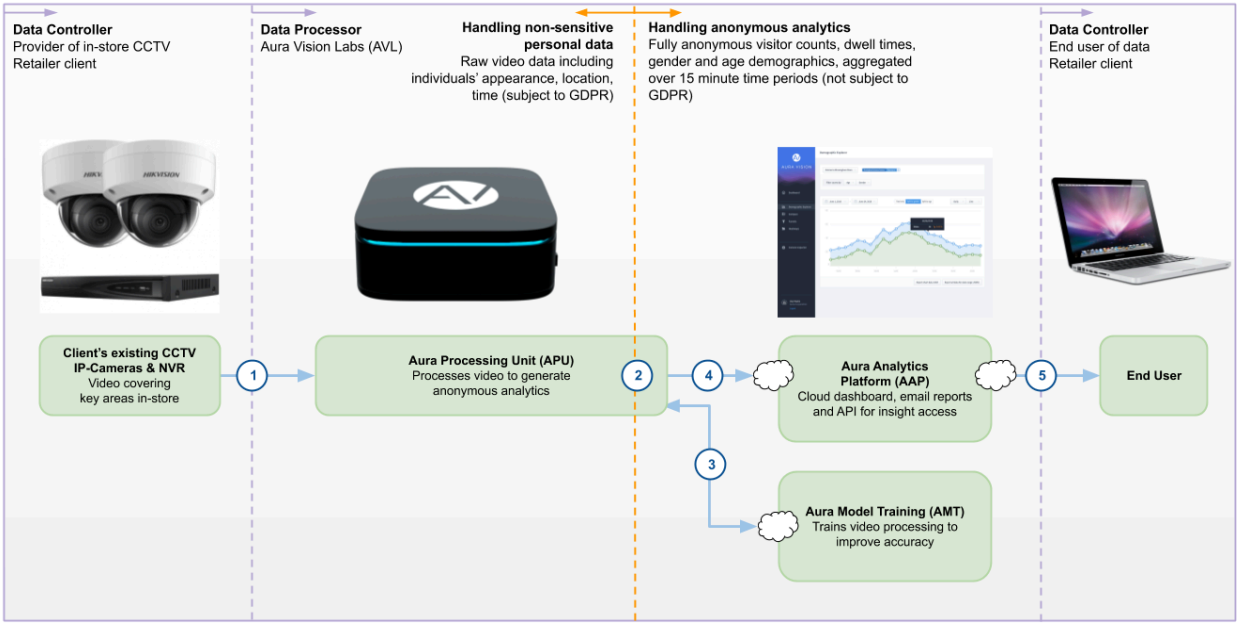
Data Controller and Data Processor

The client is the Data Controller (e.g. the operator of the retail stores, shopping mall or commercial real-estate). The operator has authority over the physical space and in-store surveillance systems (CCTV) that capture video footage and is also typically the end-user of Aura Vision's platform and insights.

Aura Vision is the Data Processor when providing its cloud platform solution, as it processes the CCTV video footage into anonymous analytics, as requested by, and on behalf of the Data Controller (the client).

Data Flow Diagram

The flow diagram below describes the data processing stages from collection of the camera data through to generation of the anonymous analytical data.



1 - Video transfer

Where video is transferred from the location's CCTV security camera system to Aura Vision's APU devices hosted on-premise.

2 - Video processing

Where APU devices employ Aura Vision's world-class AI algorithms to convert live security camera video feeds into anonymous count analytics in real-time.

3 - Snapshot transfer

Where a limited number of anonymised 'snapshot images' are transferred from APU devices to the Aura Model Training (AMT) service during initial setup, allowing Aura Vision's team of Computer Vision experts to audit and fine-tune AI models to ensure top quality analytics accuracy.

4 - Analytics transfer

Where anonymous analytics are transferred from on-premise APU devices to the cloud Aura Analytics Platform (AAP).

5 - End-user access

Where End-users access the anonymous analytics via the Aura Analytics Platform (AAP).

Feedback

We hope this clarifies how the Aura Vision AI works, but also what that means from a data protection regulatory position. If you think we have missed anything or there's anything further you'd like to know, please do let us know by reaching out to hello@auravision.ai.