AURA VISION

Data Protection Impact Assessment (DPIA)

Introduction

Aura Vision is a new solution helping brick-and-mortar retailers and shopping malls to drive sales, footfall and conversion from their physical locations, by better understanding their customers and day-to-day operations.

Who this document is for

This Data Protection Impact Assessment (DPIA) document is for anyone assessing the use of Aura Vision as an in-store analytics solution - from legal council 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.

About Aura Vision

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 lots of expensive sensor hardware to be installed.

Aura Vision is in-use in hundreds of locations all over the globe, from the UK and EU through to the US and Japan, deployed with some of the world's largest retailers.

Privacy-by-design

Since its inception in the UK in 2017, Aura Vision was built following privacy-by-design principles, adhering to the highest GDPR 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.

Contents

How it works

Aura Vision supplies a small on-premise device (APU) that is connected to each store's security camera (CCTV) system. This device processes video footage into anonymous analytics which are then made accessible via the Aura Analytics web platform (AAP).

Video footage contains images of customers and staff and is therefore classed as personal data. Video footage is maintained on-premise, and only anonymous analytics are transferred over the internet. The Aura Model Training service occasionally uses face-blurred images to validate and improve the solution's overall accuracy, these images are not classed as personal data as individuals can not be identified from them and the time and locations of images are not stored.

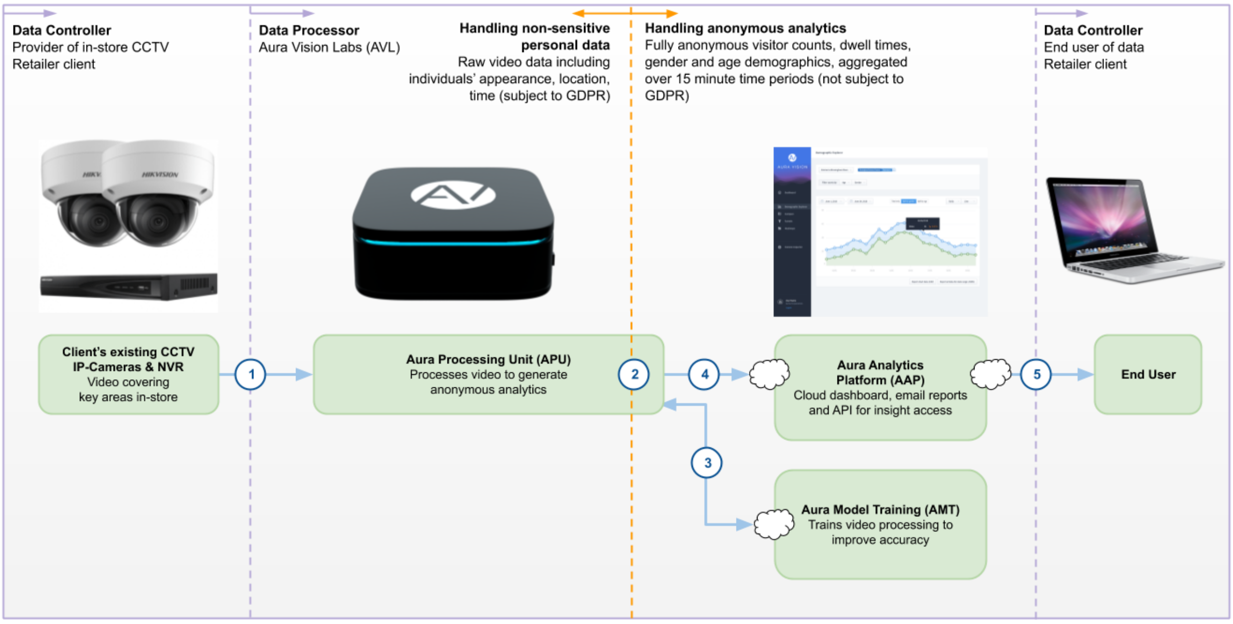
Data Controller and Data Processor

The retailer or shopping mall is the *Data Controller*, as the operator of the physical space and in-store surveillance systems (CCTV) that capture video footage.

Aura Vision is the *Data Processor*, as it processes the CCTV video footage into anonymous analytics, as requested by the Data Controller.

Data Flow Diagram

The flow diagram below overviews the data processing stages.



Data Controller
Provider of in-store CCTV
Retailer client
Data Processor
Aura Vision Labs (AVL)
Handling non-sensitive personal data
Raw video data including individuals' appearance, location, time (subject to GDPR)
Handling anonymous analytics
Fully anonymous visitor counts, dwell times, gender and age demographics, aggregated over 15 minute time periods (not subject to GDPR)
Data Controller
End user of data
Retailer client
Client's existing CCTV IP-Cameras & NVR
Video covering key areas in-store
1
Aura Processing Unit (APU)
Processes video to generate anonymous analytics
2
4
Aura Analytics Platform (AAP)
Cloud dashboard, email reports and API for insight access
5
End User
3
Aura Model Training (AMT)
Trains video processing to improve accuracy

Risk Mitigations

Stage	Type	Risk mitigation
1 - Video transfer From store’s CCTV cameras to APU	Principle (c) – data minimisation	Only those cameras which AVL and Client have agreed in advance are processed to deliver in-store analytics
	APU Security	Only AVL employee has access to APU public-private SSH keys.
	Camera Security	Only Client's designated CCTV Contractor and AVL employee have access to camera username and passwords.
	Comms Security	Cameras communicate with APU over secure connection, either direct ethernet cable or WPA2 encrypted Wifi.
	NVR Security	NVR software is not modified and its operation is not affected by AVL’s APU to avoid compromising NVR software security.
2 - Video processing Generating anonymous analytics on APU	Principle (b) – purpose limitation	AVL provides anonymous analytics only as per the Service Agreement between AVL and Client.
	Principle (e) – storage limitation	Video is immediately processed and discarded on the APU.
	Principle (f) – integrity and confidentiality	Video is processed into fully anonymised analytics, aggregated over 15 minute time periods, preventing data subjects from individuation or being linked to other data sources
3 - Snapshot transfer For manual auditing of counting accuracy and to improve the solution’s overall accuracy.	Principle (a) – lawfulness, fairness and transparency	Video snapshots are transferred only to AMT servers hosted in the EEA on Amazon AWS
	Principle (f) – integrity and confidentiality	Video is processed to blur all visible faces, removing subject identities.
	Principle (b) – purpose limitation Principle (c) – data minimisation	AVL uses video snapsh to only provide required features such as staff/customer detection and improve the accuracy if its analytics service, as per the Service Agreement between AVL and Client.
	Principle (c) – data minimisation	Only a very limited number of video snapshots are shared to AMT during the

		validation period and at infrequent periods during operation to ensure the quality of AVLs analytics service.
	Principle (e) – storage limitation	AVL stores video snapshots for a maximum of 2 weeks and discards them once model training has been performed.
	Principle (f) – integrity and confidentiality	AVL ensures that all personnel who have access to video snapshots are obliged to keep the Personal Data confidential.
	Comms Security	Video snapshots transferred using industry standard HTTPS and SSH public-private key security
	Comms Operation	APU communicates at a maximum of 20Kb/s during peak operation to minimise interference with in-store internet
4 - Analytics transfer From APU to AAP cloud	Comms Security	Anonymous analytics transferred to AAP using industry standard HTTPS security
	Comms Operation	APU communicates at a maximum of 20Kb/s during peak operation to minimise interference with in-store internet
5 - End-user access Visitor analytics via AAP	Account Security	Web platform access is controlled via username and passwords shared only with intended Client users
	Comms Security	Web platform operates over fully certified secure HTTPS protocol
Other service considerations	Principle (a) – lawfulness, fairness and transparency	Client’s customers should be made aware of CCTV filming for existing safety and security purposes, and for new store improvement purposes, with signs prominently displayed at store entrances.
	Principle (a) – lawfulness, fairness and transparency	The lawful basis for AVL to process Client's personal data is Legitimate Interest, and Client should have performed a Legitimate Interest Assessment Balancing Test (attached)
	Principle (b) – purpose limitation	Staffing insights can be optionally not stored on AAP to further protect employee privacy at Client's discretion

Legitimate Interest Assessment (LIA) Template

The lawful basis for using Aura Vision to process video footage is most often Legitimate Interest. Below we have included an LIA template for your internal use, based on the ICO's v1.0 LIA template. It is best practice to conduct an LIA to meet your obligations under GDPR's accountability principle.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

Processing customer and staff data from within retail store locations is expected to increase top-line revenue, increase real-estate value, improve brand awareness, improve marketing activities, and to optimise merchandising and store operation decisions.

The expected benefit is to help retailers and shopping malls better understand:

- which consumer audience their brand and products appeal to
- which products are driving traffic to their retail store
- which retailers are driving most traffic to their mall
- ways in which they can improve their stores to generate more sales
- ways in which they can improve their malls to drive more traffic
- return-on-investment of marketing campaigns

Without this information our clients are losing a large percentage of sales volume across every store due to mistargeted marketing and merchandising, and under-performing store layouts, or underperforming tenancy decisions for malls. In turn, this can negatively affect a company's profitability, possibly leading to long-term financial difficulty.

Video data captured from new/pre-existing security cameras in retail shopping locations will be processed to generate anonymous, privacy protecting statistics on:

- customer demographics entering the store
- where customers move within the store
- which products customers interact with and for how long
- how long customers spend in queues

Video data is processed and instantly discarded by an on-premises device supplied by AVL. Data processing generates high-level statistics that are entirely anonymous, protecting consumer privacy and identities through statistical aggregation over 15 minute time periods. No identities or personal data are stored as a result of data processing.

To improve the overall accuracy of the analytics service a very limited number of video snapshots are transferred to AVL's Model Training servers hosted in the EEA. Visible faces are blurred in all video snapshots, video snapshots are stored no longer than 2 weeks and are used only to improve AVL's service provided to the client.

Clients are advised to place clearly visible signs on store and mall entrances, to inform customers that anonymous data processing is taking place to enhance shopping experiences.

AVL complies with industry guidelines on the security, storage, transmission and processing of video information for analytics purposes as set out in our security policy and DPIA.

Wider benefits to the public will be improvements to their shopping experience inside operational stores and malls.

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

- Will this processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Our data processing methodology is designed for the specific purpose of providing retailers and malls with information on customers visiting their locations and how well their stores, products and marketing activities are performing.

No additional information is collected that will be used outside of this purpose.

This purpose can not be achieved without some form of data processing. Alternatives include:

- tracking mobile phones through a variety of technologies, all of which include tracking customer and device identities in potentially intrusive ways
- footfall counting methods, which do not offer the granularity of information to understand the full shopping journey, only providing partial information for the purpose
- loyalty card schemes, not applicable in all retail environments, and requiring explicit opt-in from all customers
- manual surveys / time and motion studies, that are often short term and limited in the depth of information they can collect

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

A DPIA Data Flow Diagram is supplied in addition to this LIA, as video data containing personal identities is processed in order to generate anonymous visitor statistics.

No sensitive personal data is processed, and the processing has the ability to exclude childrens' and staff data at the Client's discretion.

Reasonable expectations

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Data is processed only from customers entering the store. The Client is to place prominent signage at store entrances, informing customers of the data processing in progress and the reasons for it.

No data is not obtained from a third party, and video data is never shared with third parties.

While this data processing solution is an innovative way to collect such information, customers are already accustom to other more traditional data collection methods such as loyalty cards, surveys or time and motion studies conducted by market research agencies.

Likely impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

The impact on customers should be minimal as processed data is entirely anonymous and does not store or link to customer identities. Furthermore, it is not being acted on in real-time, and no autonomous decisions are being made as a result of the data collected.

Processed data is for use in longer-term planning and strategy management, rather than to influence customer behaviour by targeting an individual.

Individuals should not lose control over their personal data, as clear signs are to be placed on entrance informing customers on the data processing taking place, before they enter the premises. Information like gender, age and location within the store are already readily available to be recorded via other surveying methods.

Individuals can opt-out of data processing, such that for the time they are in the store, no video data is processed, and generated statistics are discarded.

Can you offer individuals an opt-out?	Yes / ~~No~~

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes / ~~No~~

A clear purpose is identified, with positive outcomes for the business, and potentially very negative outcomes if not performed.

A clear necessity is identified, with other solutions requiring much more intrusive methods, or not providing adequate information for the purpose.

The balancing test indicates that:

- no sensitive personal data is processed
- customers are informed of the data processing activity such that it is a reasonable expectation once a customer enters the store
- the likely impact on the customer is minimised through data anonymisation and ability to opt-out

LIA completed by	Daniel Martinho-Corbishley
Date	29th September 2019

What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.