Airport Retailers Association

ARA

Data Protection Impact Assessment (DPIA)

2024-2025

contact@veesion.com

DATA PROTECTION IMPACT ASSESSMENT

1. Background study

1. 1. Overview

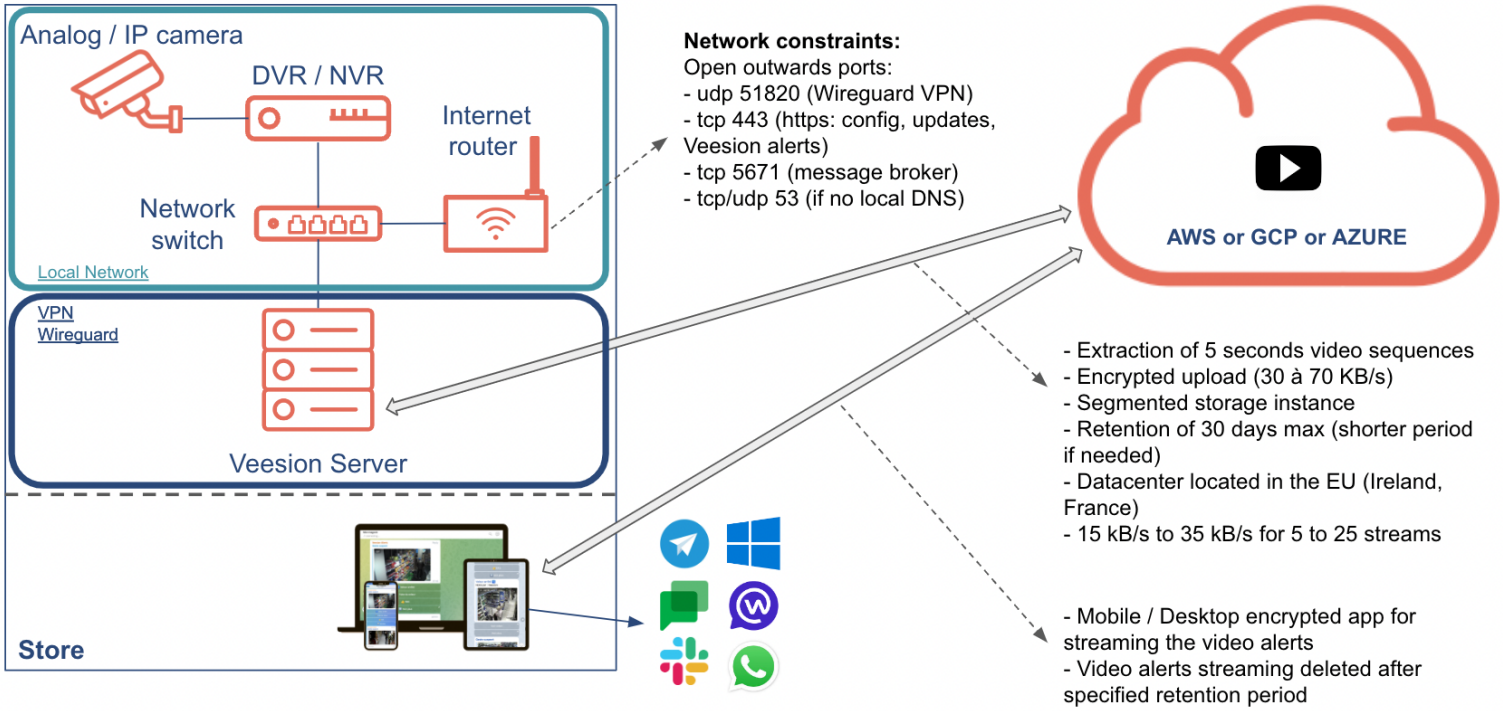
Description of the processing	Veesion Run® is a gesture recognition technology. It allows the analysis of video surveillance feeds from a point of sale in order to automatically detect gestures associated with shoplifting: - Concealment of an item in the upper body - Concealment of an item in the lower part of the body - Concealment of an item in a personal bag
Purposes of the processing	Protection of goods and people.
Stakes of the processing	Creation of a new service: detection of gestures associated with theft and transmission of video sequences containing these gestures to point-of-sale employees.
Person in charge of the processing	Client
Subcontractor(s)	• Veesion • Amazon Web Services (AWS)

1. 2. Data, processes and media

Description of data, recipients and retention periods

Collected data	Recipients	Shelf life
Username / password of a user account of the video protection recorder	Veesion	Until deletion is requested by the controller.
Video extracts from the video protection system (Video alerts)	Client	1 to 30 days according to prefectural recommendations and customer request

Description of processes and supports



Processes	Description	Data storage
Analysis by the algorithm	A Veesion server deployed locally at the processor's site is connected to the DVR (Digital Video Recorder) or NVR (Numerical Video Recorder) via ethernet. The server contains the gesture detection algorithm and continuously analyzes in real time the video streams of the point of sale video protection system.	Veesion Server
Video alerts transmission	The algorithm detects the gestures associated with theft: hiding in the upper part of the body, hiding in the lower part of the body, hiding in a bag, etc... When the algorithm has detected a gesture associated with potential shoplifting, a video sequence is extracted ("video alert"), and then transmitted to a secure, segmented cloud storage instance.	Cloud Server
Transmission of valid video alerts	Video alerts are accessible from an end-to-end encrypted messaging application as a clickable link at the point of sale on mobile or server.	Device dedicated to the reception / consultation of video alerts belonging to the controller.
Suppression	Alerts stored on cloud storage after 1 to 30 days. They can be deleted within a shorter period of time upon request of the customer.	Cloud Server

2. Study of the fundamental principles

2. 1. Assessment of measures to ensure proportionality and necessity of the processing

Explanation and justification of purposes (art.5.1 (b))

Goals	Legitimacy
The data is collected to provide the service requested by the controller, which is to **analyze video surveillance feeds to help identify actions associated with potential shoplifting.**	**Legitimate interests: ensuring the safety and protection of individuals and property.** The purpose of collection for the provision of the service requested by the data controller is specific, explicit and legitimate: Protection of property and persons.

Explanation and justification of the minimization (adequate, relevant, not excessive) of data (art.5 (c))

Details of processed data	Justification of the need and relevance of the data	Minimization measures
Video alerts.	The data needed to deliver the service is minimized before being transmitted to the cloud server. • Only the data necessary to provide the service are collected and analyzed. • Only this data is kept and for a period of time in accordance with the regulations in force.	The retention period of the video alerts respects the duration recommended by public institutions and the GDPR (15 or 30 days).

Accurate and up-to-date data (s.5.1 (d))

Not applicable

Explanation and justification of retention periods (art.5.1 (e))

Types of data	Shelf life	Justification of the shelf life	Deletion mechanism at the end of the retention period
Analyzed data Video alerts	1 to 30 days.	The retention period respects the duration recommended by the prefecture. The video alerts are therefore accessible a posteriori by the data controller if he expresses the need (as are the recording tapes of the video protection system).	On demand, video data is made unreadable and cloud storage areas that have been used are erased and overwritten. They are then no longer accessible on any medium whatsoever.

Evaluation of measures

Measures to ensure proportionality and necessity of processing	Acceptable / improvable?
Purposes: determined, explicit and legitimate	Acceptable. The sole purpose of the service provided by Veesion to the data controller is the same as that of the video protection system.
Basis: lawfulness of processing, prohibition of misuse of purpose	Acceptable. The processing concerns data strictly necessary for the provision of the service. It involves professional remote monitoring operators
Data minimization: adequate, relevant and limited	Acceptable. The need for video data collection is obvious.
Data quality: accurate and up-to-date	Acceptable.
Shelf life : limited	Acceptable. The retention period does not exceed 30 days and is adjustable according to the request of the data controller.

2.2 Evaluation of the measures protecting the rights of the persons concerned

Determination and description of measures for the information of persons (art.12)

Measures for the right to information	Methods of implementation	Justification of the modalities or impossibility of their implementation
Presentation of the conditions of use / confidentiality	Possibility of putting up a poster at the entrance of the point of sale.	When the point of sale is equipped with a video protection system, a sign informing customers must already be displayed at the entrance. A mention specifying the nature of the processing carried out by Veesion may be added.
Possibility to access the terms of use / privacy.	On customer request.	The customer can already request information on the site's video protection.
Readable and understandable conditions.	Yes.	
Existence of clauses specific to the device.	Yes.	
Detailed presentation of the purposes of the data processing (precise objectives, cross-referencing of data if applicable, etc.).	On customer request..	
Detailed presentation of the personal data collected.	On customer request.	

Determination and description of measures for the collection of consent (art.7)

Not applicable.

Determination and description of measures for subcontracting (art. 28)

Name of the subcontractor	Purpose	Perimeter	Contract reference	Compliance contract art.28
Amazon Web Services (AWS)	Private cloud hosting.	Hosting of video alerts.		

Determination and description of measures for the transfer of data outside the European Union (chap.5)

Datas	France	EU	Country recognized as suitable by the EU	Other countries	Justification and framework (standard contractual clauses, internal company rules)
Video alerts	Yes	Yes	No	No	Datacenter of the cloud host located in the EU.

Evaluation of measures

Measures to protect the rights of the persons concerned	Acceptable / improvable?
Information to data subjects (fair and transparent processing)	Acceptable. An explicit and immediately visible display in the reception area of the establishment is already in place. It is then possible to add a document on the service delivered by Veesion to inform clients.
Collection of consent	Not applicable (legal basis is legitimate interest).
Exercising access and portability rights	Acceptable. The only data accessible by Veesion and more specifically by the professional remote surveillance operators assigned to their classification are the video alerts extracted from the video protection system. The data controller can retrieve them in their entirety upon request of the end customer. The client can request access to all the video alerts on which he appears. The customer can already ask for access to the video extracts of the video protection system on which he appears and this, under certain conditions.

Exercise of the rights of rectification and deletion	Acceptable. The data controller may request the erasure of all data collected by Veesion in connection with the provision of the service, prior to the maximum retention period of 30 days if necessary. An acknowledgement of receipt is sent to confirm that the request has been taken into account.
Exercise of the rights to limit processing and to object	Acceptable. At any time, Veesion may suspend the processing of data necessary for the provision of the service, for the time necessary to verify the validity of a request from the data controller or a client of the data controller.
Subcontracting: identified and contracted	Acceptable. AWS acts as a subcontractor. A subcontracting agreement is concluded between the 2 companies specifying all the elements provided for in art. 28 (duration, scope, purpose, documented processing instructions, prior authorization in the event of recourse to a subcontractor, provision of all documentation providing proof of compliance with the Regulation, immediate notification of any data breach, etc.).
Transfers: compliance with obligations regarding the transfer of data outside the European Union.	Acceptable. No data is transferred outside the EU.

3. Study of the risks related to data security

3.1 Evaluation of measures

Description and assessment of measures to help address data security risks (art.32)

Measures specific to the processing data	How to implement or justify otherwise	Acceptable / improvable?
Encryption	All connections, between the video protection system, the local server, the cloud server and the device used to display the alerts, are done in SSL via the https protocol. The https protocol used is based on RSA 2048 with TLS v1.2.	Acceptable.
Anonymization	Not applicable. Video alerts are viewed by professional security guards who are authorized to view recordings from a video protection system.	Not applicable.
Data compartmentalization (with respect to the rest of the information system)	The cloud solution chosen by Veesion offers isolation from the data of other customers of the service.	Acceptable. Customer data is isolated from each other in the servers used by Veesion. The instances on which the servers run are dedicated and cannot be used by third parties.
Logical access control	By username (nominative) and password. It is Veesion's responsibility to maintain the confidentiality of this connection information.	Acceptable. Veesion modifies the logical accesses to the platform dedicated to the classification of video alerts every week. The platform is only accessible from a local Veesion server, therefore only during the hours dedicated to providing the service. Access is based on authentication mechanisms that meet current security standards (SSHv2 with RSA 4096 key).
Archiving	The data is kept for 1 to 30 days as are the recordings from the video protection system. At the end of	Acceptable. The duration of conservation respects the duration decided

	the retention period or upon request, the data is rendered unreadable and the storage areas that have been used are erased and overwritten. For the erasure process to be effective, Veesion distinguishes between data in the local server deployed at the point of sale, the cloud server and the mobile device used to display video alerts.	by the prefect and is fixed according to what is strictly necessary for the good functioning of the service.
Paper document security	Not applicable	

Description and evaluation of general security measures

General security measures of the system in which the processing is carried out	How to implement or justify otherwise	Acceptable / improvable?
Safety of the operation	Cloud server maintenance is covered by the contract with the chosen cloud provider. Local server maintenance is covered by Veesion. Security assessment of providers: A security questionnaire will be distributed to potential providers to check their compliance with the RGPD.	Acceptable.
Fight against malware	Server maintenance is covered by the contract with the chosen cloud provider. The maintenance of the local server is covered by Veesion.	Acceptable.
Workstation management	Workstation security is guaranteed by Veesion's security policy.	Acceptable.
Web site security	The security measures implemented when using a cloud server are described in the security policy of the chosen cloud provider.	Acceptable.
Backups	Performed in the local server and the cloud server.	Acceptable.
Security of computer channels (networks)	The following networks are implemented: - Private network of the point of sale equipped via VPN Wireguard;	Acceptable.

	- Internet ; - private cloud network. The private network of the equipped point of sale is already secured.	
Monitoring	The security measures implemented when using a cloud server are described in the security policy of the chosen cloud provider.	Acceptable.
Physical access control	The access control measures implemented by the chosen cloud provider for access to its infrastructure are described in its security policy. Access control measures that meet current security standards are already implemented by the controller.	Acceptable.
Safety of materials	The security measures implemented when using a cloud server are described in the security policy of the chosen cloud provider. Security measures that meet current security standards are already implemented by the controller.	Acceptable.
Removal of sources of risk	The security policy of the chosen cloud provider mentions the attention paid to natural hazards when choosing the location of their datacenters.	Acceptable.

Description and evaluation of organizational measures (governance)

Organizational measures (governance)	**How to implement or justify otherwise**	**Acceptable / improvable?**
Organization	Access to personal data by Veesion employees requires authorization. The client's employees have nominative access to the video alerts.	Acceptable.
Risk management	The potential risks that the processing carried out by Veesion pose to the privacy of the persons concerned are the same as for a traditional remote surveillance service. These potential risks are limited by the implementation of measures / protocols in the analysis, transfer and processing of video alerts. These	Acceptable.

	measures comply with current security standards.	
Incident and data breach management	In the event of an incident, the following measures are put in place: - Veesion notifies the group of the occurrence of an incident via an email to the designated individuals. The email describes the incident as fully as possible and is sent within 24 hours of the incident. - All user accounts are deleted or will have their passwords changed depending on the severity of the incident. - 2 network engineers are mobilized to identify the source of the incident, its nature and its level of severity. - An intermediate incident report is sent to the designated persons via email. This report gives the information collected by the network engineers. - Once the incident is closed, a final incident report is sent to the designated persons via email. This report presents the incident in its entirety (source, nature, actual and potential consequences) as well as the measures that were taken to remedy it.	Acceptable.
Personnel management	Included in the contract with the provider is: - Awareness measures taken when a person arrives in his or her position - Measures taken when people accessing the data leave: In case of departure of staff accessing personal data, their account is instantly deactivated.	Acceptable.
Relations with third parties	The terms of access to the data are specified in the subcontract with AWS.	Acceptable.
Supervision	A Veesion employee is responsible for ensuring the proper delivery of the service by the subcontractor and performs internal audits: verification of the implementation of security clauses, audit of all accesses and user	Acceptable.

	accounts used by the subcontractor as well as its activity (personnel changes, network event logs).	

3.2 Risk Assessment: Potential Privacy Breaches

Risk analysis and estimation

Risks	Main sources of risk	Main threats	Main potential impacts	Main measures reducing severity (G) and likelihood (V)	G	V
Illegitimate access to data	Veesion employee Attacker Customer	Veesion employee Attacker Customer	Consequences of communicating potentially sensitive information, such as video footage of a theft: risk of defamation of the person, (discrimination, threats, aggression, loss of employment, loss of access to services, etc.)	Retention periods from 1 to 30 days. Physical / logical access control. Encryption of flows by the cloud provider via RTSP protocol. Access traceability. Very high security standards of the cloud provider.	Important	Limited
Unwanted modification of data	Veesion employee Attacker Customer	Data corruption on the local server Data corruption on the cloud	Deterioration of the quality of service delivered by Veesion	Double backup (cloud server backup, local server backup) Encryption of data flows by the cloud provider via RTSP protocol Physical / logical access control.	Limited	Limited
Disappearance of data	Veesion employee Attacker Customer	Data deletion (via cloud or server) Physical damage or degradation of servers	Need to replace the local server Deterioration of the quality of service delivered by Veesion	Double backup (cloud server backup, local server backup) Encryption of data flows by the cloud provider via RTSP protocol Physical / logical access control.	Limited	Limited

Risks	Acceptable / Improvable?
Illegitimate access to data	Acceptable. Data could still be stolen by an employee of Veesion or of the customer, in order to characterize a situation that is relevant to the private life of the persons (e.g. adultery, flagrant theft, etc.). The risk of defamation of the person already exists within the framework of a classic remote monitoring without the service delivered by Veesion. However, the customer's employees are professionals and the legal consequences can be dissuasive.
Unwanted modification of data	Acceptable. A customer's video alerts are distorted/replaced due to a hack or error and the customer observes a deterioration in the quality of service. The risk seems acceptable in terms of severity (Limited) and likelihood (Limited) and, given the security measures in place.
Disappearance of data	Acceptable. A customer's video alerts are deleted due to a hack or error and the customer observes a deterioration in service quality. The risk appears to be acceptable in terms of residual severity (limited) and likelihood (limited), given existing or planned measures. The original recording tapes from the existing video surveillance system are not at greater risk with the processing done by Veesion.