



February 2025

To Whom It May Concern

GDPR Compliance

As a company we are aware of our responsibilities under GDPR and have prepared the following self-declaration to demonstrate what actions we have taken towards compliance with regard to our Vaidio™ AI Vision Platform.

Privacy Protection

- Privacy Protection, if activated, automatically blurs all detected persons and faces in search and alert results throughout the Vaidio UI, regardless of which AI engines are activated.
- Privacy Protection allows authorized users to unblur certain detected faces / persons on demand for investigative purposes.
- In the expanded view of the video search results authorized users can select Masked Video Export, which will mask the faces and license plate numbers found in the playback video clip.

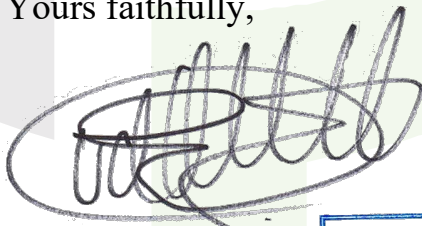
User Management

- User Management allows Vaidio Administrator to create User Groups, add New User Accounts to each User Group, and assign Privileges to each User Group.
- Vaidio Administrator can assign the following types of Privileges via User Management: camera control; video source control; AI engine control; configuration control.
- Vaidio Administrator is able to manage the system, activities, and user groups via user permission.

Data Security

- On-premise deployment: Vaidio connects to the cameras and NVRs in the LAN and operates within the network security of the LAN.
- Cloud deployment: Vaidio operates within the network security of the cloud instance, e.g. Amazon Web Services (AWS)
- Vaidio utilizes the HTTPS protocol to transmit sensitive information over a TCP/IP network from user workstations to the server.
- The HTTPS protocol uses Secure Socket Layer (SSL) to encrypt data that is transferred between client and server. SSL uses the RSA algorithm, which is an asymmetric encryption technology. Vaidio uses 256-bit AES encryption over networks and from servers to browsers.
- Vaidio utilizes the following data encryption types: *per column encryption* for sensitive data; *disk encryption* to prevent unencrypted data from being read from the drives if the drives or the entire computer is stolen.
- Vaidio Administrator is able to set the desired data retention time (number of days to save data in the Vaidio appliance).
- Vaidio user access to allow read-only access, update access, or no-access to specific types of records, record attributes, components, or functions.
- Vaidio system log for analyzing specific trends or record the data-based events / actions of the Vaidio system environment.
- Vaidio diagnostic log registers hardware errors, processing consumption, analytic / alert / connection errors, failed login attempt from the IP address of the computer trying to access Vaidio.
- Vaidio audit trail registers successful user login/logout, time and user actions in the entire Vaidio system (such as camera activation / modification).

Yours faithfully,



Aicuda Technology
John van den Elzen
Managing Director



johne@aicuda.world

(+31) - (0) 6 400 121 00

Ketelven 2 - Veghel - 5464 PS - The Netherlands

info@aicuda.world

www.aicuda.world