# VISOR Data Protection: Strategy and Evaluation

**Data Protection Strategy**

VISOR envisions the experimentation with federated machine-learning (ML) techniques over a mesh of IoT devices for the purpose of instrumenting smart crowd management (e.g., distributed dangerous object recognition, people trajectory tracking, as well as boundary-events recognition).

The experimentation in question is set to take place in the context of the PaasPop event (see here: <https://www.paaspop.nl/>) where the ML federation will run a total of 12 scene recognition scenarios which may include data-processing over data for which GDPR restrictions apply. In the context of such potential restrictions, the VISOR teams envisions:

1. To enact the privacy policy under the terms and conditions already agreed upon by attendees to the event (see here: <https://www.eventwarehouse.nl/privacy.php>);
2. In line with GDPR restrictions, to maintain data (in a format which is 100% anonymous at the source) for a period of up to 90 working days after the event is over; the anonymized-at-the-source form will be functional to further analysis and for research and post-processing purposes only; in synthesis, all digital data will be stored on institutional servers, which are backed-up automatically and daily. Some data may also (temporarily) be stored on departmentally owned computers that are also backed-up daily with warranty that all data is stored no longer than the period highlighted above.
3. In line with GDPR restrictions, to identify all data pertaining to children (underage people) and immediately discard said data upon elicitation;
4. To gather, store, and process the data using private/owned cloud/infrastructure/hardware and under the aforementioned restrictions;

More specifically, with respect to article 1 and 2 from the above enumeration, the VISOR team commits to conduct experimentation within the allowance already agreed upon by event attendees who, according to the PaasPop privacy policy statement Sec. “Agreement by purchasing tickets”, bullet 3, line 2, namely “To provide services based on your location”. That is, assuming that the attendees already allow location-based services provisioning, the VISOR teams offer the research and security experimentation as-a-service and within the context of pre-made scenarios in the context of the VISOR project.

**Information concerning Festival Attendees**

Festival attendees are not expected to engage in any specific participatory action with respect to VISOR activities and are intended as *co-participatory*, meaning that the VISOR experimentation will capture their likelihood and appearance as well as circumstantial information concerning their participation in the event (trajectories, clothing) for the sole purpose of smart event management and maximization of event security and safety as well as crowd management in the context of said event.

**Consistency with respect to Algemene Verordening Gegevensbescherming**

**(AVG)**

In the scope of the VISOR experimentation, only JADS researchers are intended and explicitly allowed to participate, engage in, experiment with, and in any way interact with the VISOR equipment and experimental material in the context of the research project and no volunteers are asked to participate directly. No data is stored which could identify participants of PaasPop and only fully-anonymous data is stored after processing of the videos and telemetry gathered in the context of the field study – this policy document was revised and the conclusion is that the strategy herein is AVG-compliant.