



GDPR & Videosurveillance

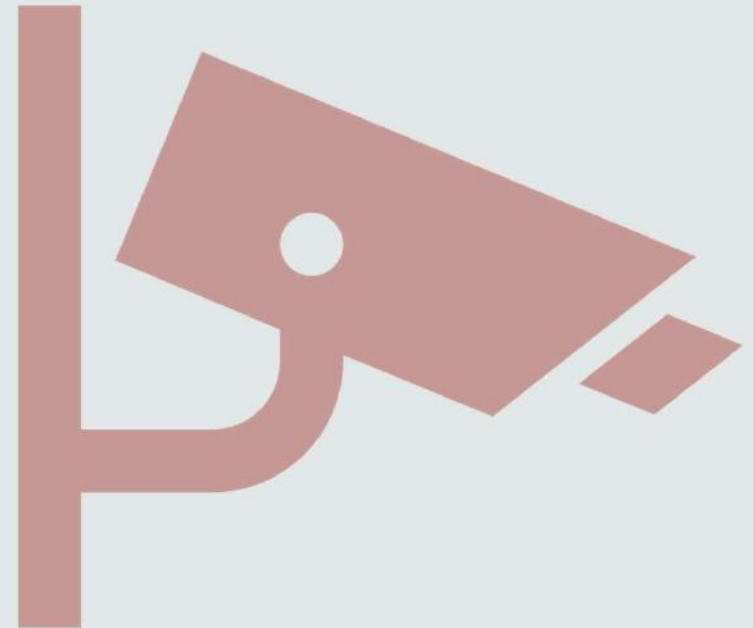
Francesco Capparelli
Italian Institute for Privacy

The legal framework: the processing of video footage and biometric data

The regulatory provisions and, more generally, the applicable legal framework may therefore vary depending on the use of video surveillance technologies, according with the specific purposes pursued.

This is because, the processing of personal data is massive and when dealing with these technologies

- especially when using facial recognition systems
- regardless of the experimental use, the provisions belonging to....



Legal Framework

- Regulation (EU) 2016/679 («GDPR»);
- Directive (EU) 2016/680 («Law Enforcement Directive» or «LED») and
- Related guidelines, recommendations, best practices, opinions and binding decisions of the EDPB are applicable.





Video surveillance and processing of video footage

- In order to achieve the objectives pursued in the context of the Project, Article 6(1)(c) of the GDPR applies when national law provides for an obligation to carry out video surveillance, in this case, it will be essential **to check the national law of the Member States concerned.**
- **Article 6 (1)(e) of the GDPR** (need to perform a task in the public interest or for the exercise of official authority);
- **Article 6 (1)(f) of the GDPR** (legitimate interest).
- For the fulfilment of the purposes, the legitimate interest (for the processing of images by means of video-surveillance tools) may be considered to coincide with the need to ensure the safety and security of Public Transport Operators («PTO») assets, as well as the safety and security of persons having access to public transport services.



The legal framework: the processing of video footage and biometric data

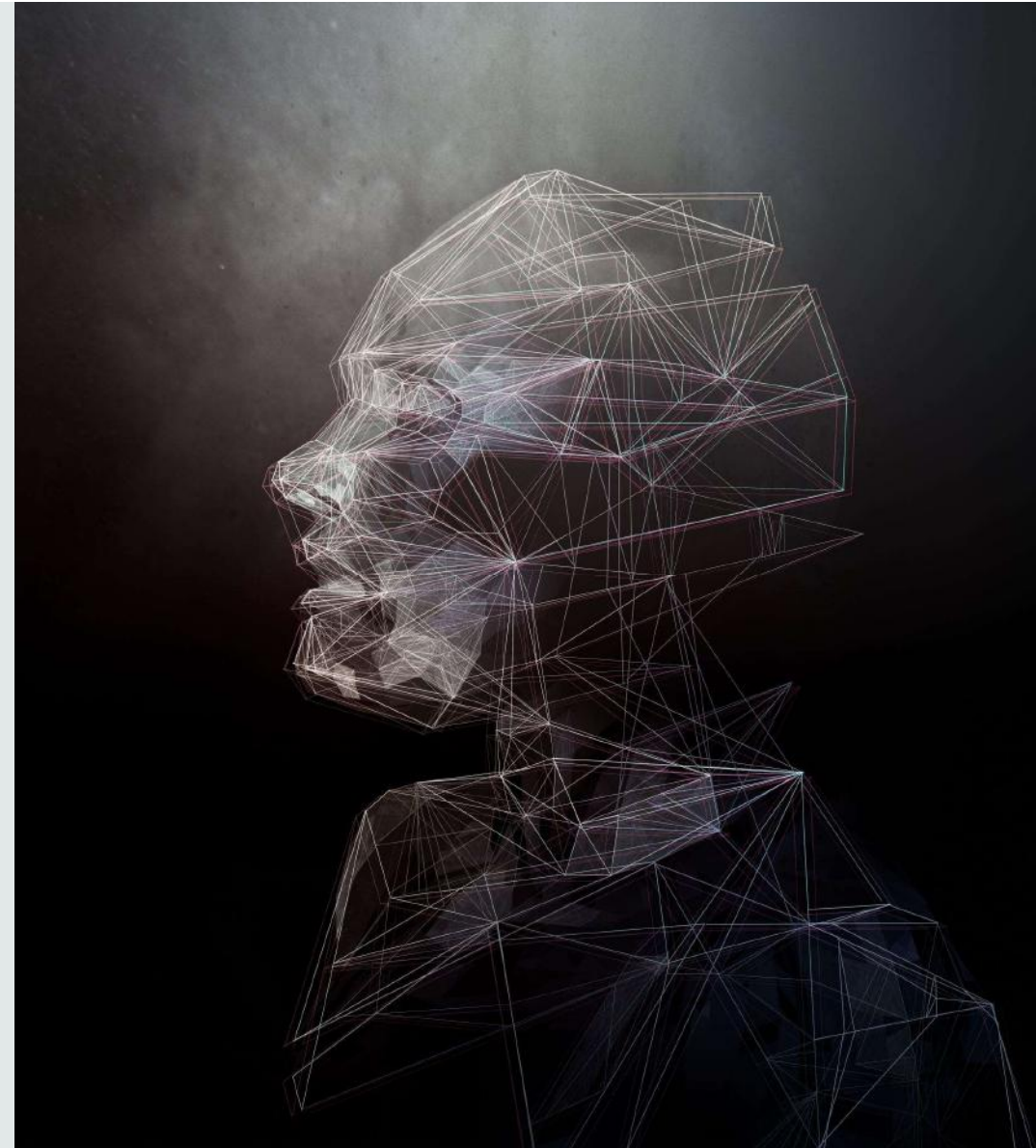
The video surveillance and the processing of biometric data

Alongside the processing of personal data relating to video-surveillance activities, it is of fundamental importance to understand when we are dealing with the processing of biometric data.

Biometric data allows the identification of a data subject at any time based on a specific biological characteristic, which is permanent (except in special cases) over time and from which the data subject cannot be dissociated.

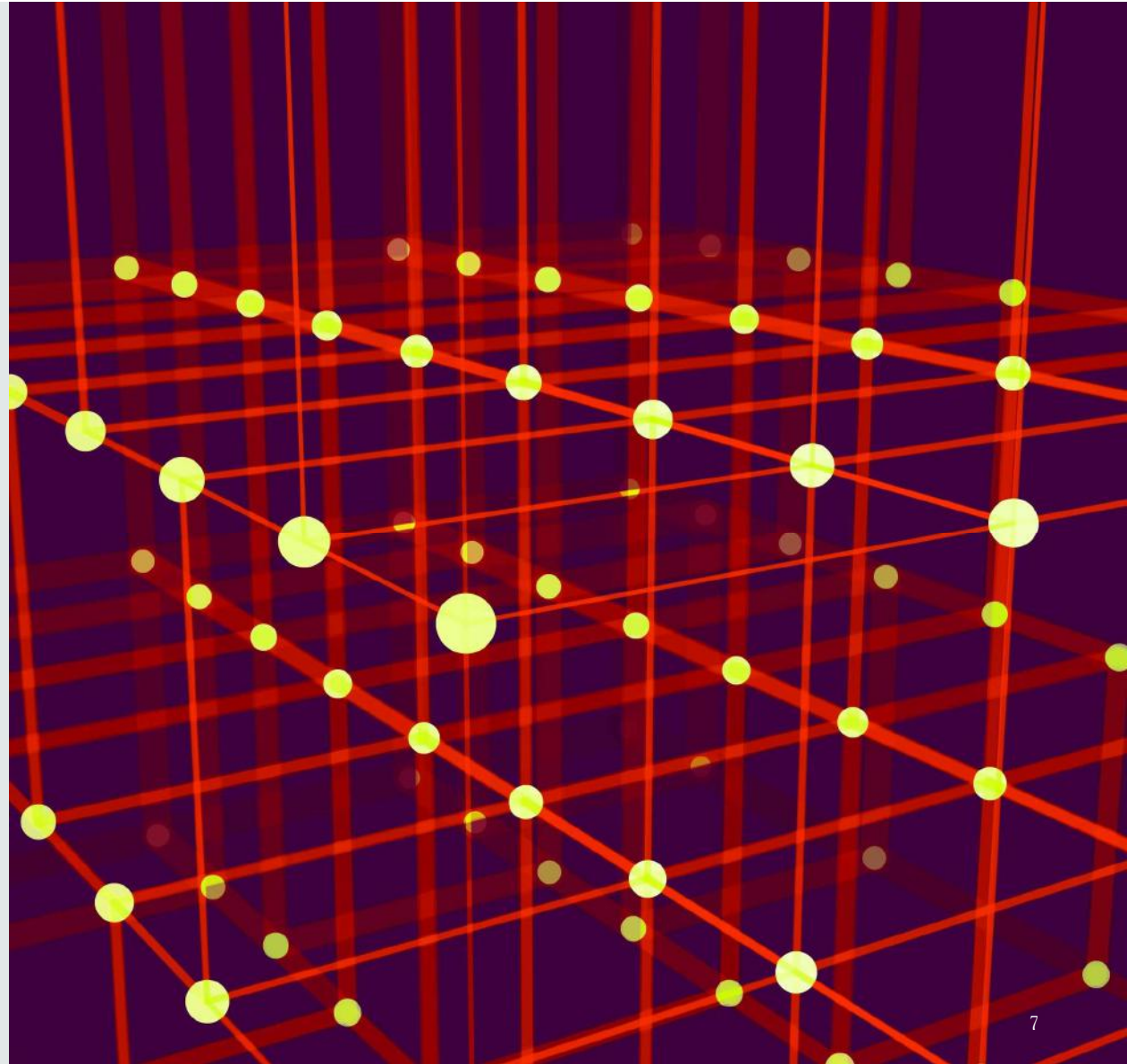
Facial Recognition

- The **facial recognition**, for example, falls under the category of "*biometric technology*".
- Biometrics includes all automated processes used to recognise an individual by analysing their physical, physiological or behavioural characteristics
- they allow or confirm the **unique identification** of a particular person.
- The GDPR equates biometric data as "sensitive" data, just like the data listed by Article 9 of the GDPR.



Necessity to perform a DPIA

- Depending on the processing activities that will have to be carried out in order to achieve compliance with the framework, a Data Protection Impact Assessment ("DPIA") will have to be carried out.
- **Article 35(1) of the GDPR** provides that data controllers are required to conduct a DPIA where the type of data processing is likely to present a "*high risk to the rights and freedoms of natural persons*".
- **Article 35 (3)(c) of the GDPR** states that data controllers are required to conduct a DPIA if the processing constitutes systematic monitoring of a large-scale publicly accessible area. Furthermore, according to **Article 35(3)(b) GDPR** a DPIA is also required when the data controller intends to process special categories of data on a large scale.





High Risk

- Furthermore, **Article 35(4) GDPR** requires each supervisory authority to publish a list of the type of processing operations that are subject to a mandatory DPIA in their Country. It is reasonable to assume that many video surveillance cases will require a DPIA.
- In case the results of the DPIA indicate that the processing would entail a high risk despite the security measures foreseen by the data controller, then it will be necessary to consult the competent Data Protection Authority prior to the processing, following the indication provided by **Article 36 of the GDPR**.




Duty to inform

- Another important legal requirement to be taken into account is the **duty to inform data subjects about the processing of their personal data**. Data subjects must be informed about the fact that video surveillance systems are in operation and about which locations are being monitored. **Transparency** and **information notice obligations** are prescribed by **Article 12 et seq. of the GDPR**. Further details are set out by the WP29 in the «*Guidelines on transparency under Regulation 2016/679 (WP260)*» approved by the EDPB on 25 May 2018.
- In line with WP260 para 26, Article 13 of the GDPR, applies if personal data is collected "[...] from a data subject by observation (e.g., using automated data capture devices or data capture software such as cameras [...])". In these circumstances, it is certainly useful to use a **layered approach**. As far as video surveillance is concerned, the most important information should be displayed on a sign (**first layer**) while other mandatory details can be provided by other means (**second layer**)".

Duty to provide an information notice under Article 13 GDPR

Example (non-binding suggestion):



Video surveillance!


Identity of the controller and, where applicable, of the controller's representative:

Contact details, including of the data protection officer (where applicable):

Information on the processing that has the most impact on the data subject (e.g. retention period or live monitoring, publication or transmission of video footage to third parties):

Purpose(s) of the video surveillance:

Data subjects rights: As a data subject you have several rights to exercise, in particular the right to request from the controller access to or erasure of your personal data.
For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.



Further information is available:

- via notice
- at our reception/ customer information register
- via internet (URL) ...

In order to comply with the requirements of **Article 12(7) of the GDPR**, the information shared should be provided **in combination with an icon** in order to give, in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. The format of the information should be adapted to the individual location (WP89 para. 22).



The purpose of the Project and its steps

- In order to effectively pursue its objectives, PREVENT PCP project will use video-surveillance systems to **PREVENT unattended items in public transport environment by detecting them and instantly track their owner(s)**. To achieve this purpose the following 3 steps/objectives shall be considered:

- 1) the ***detection of unattended items***;
- 2) the ***association between objects (luggage, bags or other) and their owner***;
- 3) the ***owner tracking once the item is left unattended***.

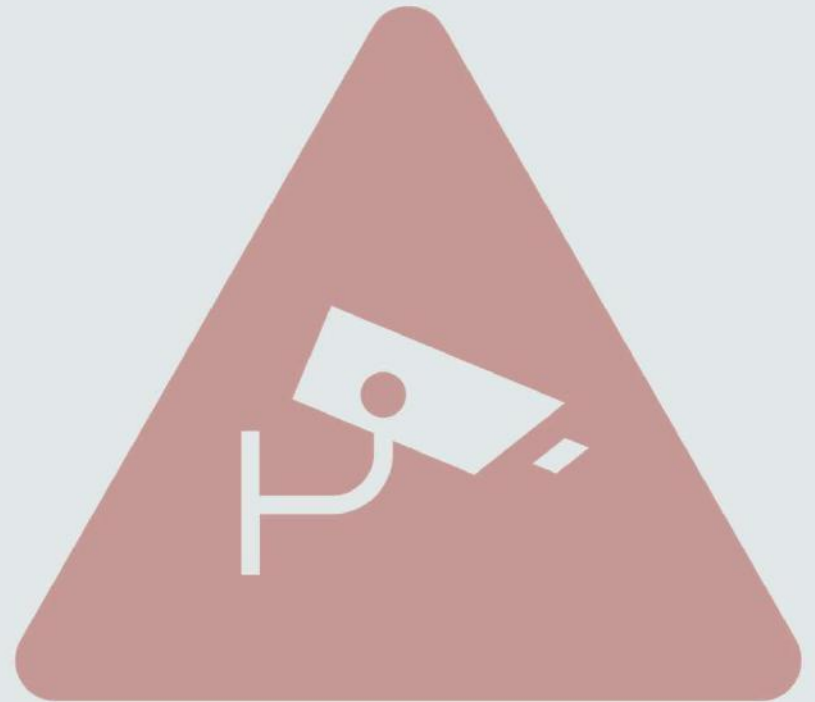
The purpose of the Project and its steps



- The precise definition of the three objectives is essential in order to assess the type of data processed - whether video footage or biometric data - and the related legal basis for processing.
- According to **Article 5(1)(b) of the GDPR**, the purposes of the processing must be specified in detail. In addition to this provision, the purposes of video surveillance must be documented in writing pursuant to **Article 5(2) of the GDPR** and must be specified for each surveillance camera in use.
- Pursuant to **Article 13 of the GDPR** and in accordance with the principle of transparency, data subjects must be informed of each of the purposes of processing implemented by the data controller.

Importance of Compliance with Data Protection Law and Cybersecurity

- Adoption of technical and organizational measures as per article 32 of the GDPR.
- Ensuring security of personal data during video surveillance.
- Aligning with principles stated in Article 5 GDPR during all processing stages.



Data Protection by Design and Default

1

Integrating data protection into technological design and organizational practices.

2

Management frameworks to establish video surveillance policies and procedures.

3

Technical system specifications include GDPR principles (like data minimization, integrity, and confidentiality).



Technical & Organizational Security Measures

- Securing video surveillance during storage (data at rest), transmission (data in transit), and processing (data in use).
- Evaluation of technology providers and their offered solutions for compliance.
- Implementing privacy-friendly technologies, e.g., masking irrelevant areas, editing out third-party images.

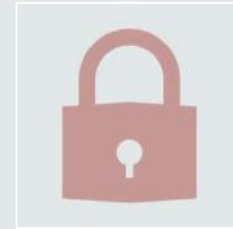
Biometric Data Processing



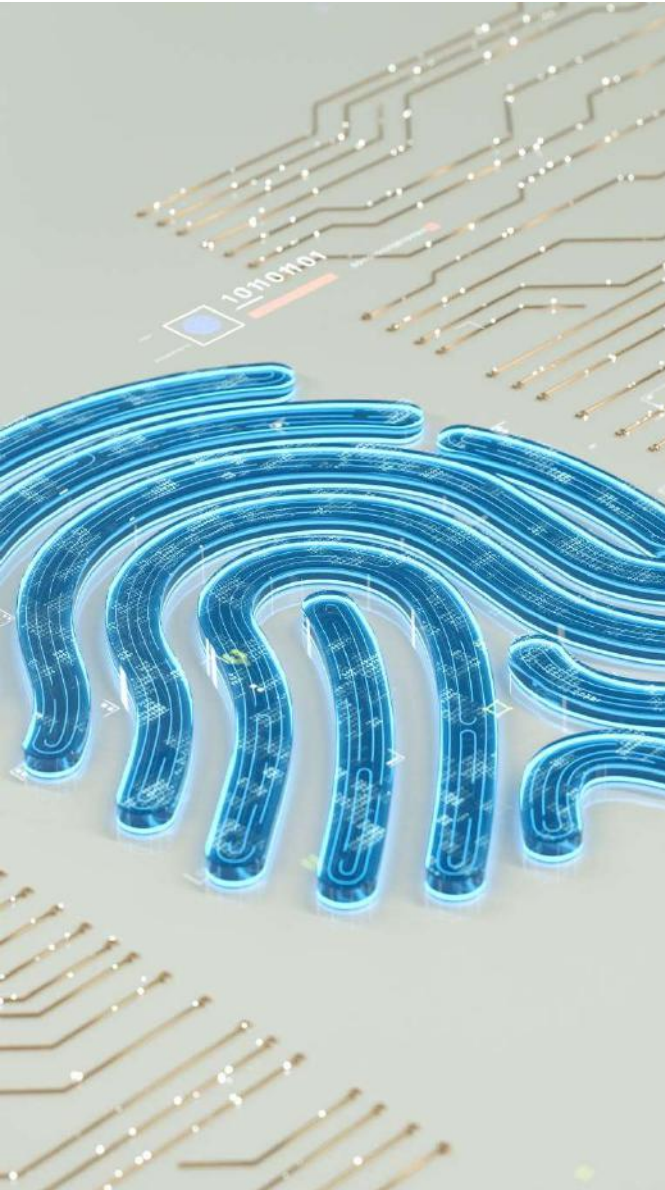
Minimizing risks associated with biometric data processing.



Considerations for storing biometric templates in centralized, encrypted databases.



Ensuring biometric data cannot be transferred across different systems.



Data Integrity, Deletion, and Unauthorized Access

- Maintaining data availability, integrity, and confidentiality.
- Measures such as compartmentalizing data, encrypting biometric data, and fraud detection.
- Immediate deletion of raw data when there's no lawful basis for processing and exploring noise-additive methods.

Conclusion



Q&A



DEBATE



DOUBTS AND
CLARIFICATIONS