CLIENT MEMO

New Regulation on Processing of Personal Data through Video Surveillance systems

January 27, 2020

On January 16, 2020, Directorial Resolution No. 02-2020-JUS/DGTAIPD, which approved the Directive for Processing of Personal Data through Video Surveillance systems (the "Directive") was published. The Directive is complementary to what is established under Law No. 29733, Personal Data Protection Law (the "PDPL") and its corresponding regulation, approved through Supreme Decree No. 003-2013-JUS.

A summary of the Directive's principal aspects is featured below:

1. What is a video surveillance system?

A video surveillance system consists of a group formed by one or more persons and technological devices (composed of one or more interconnected and strategically placed cameras) that involve the treatment of personal data.

2. What cases are covered within the scope of this Directive?

The Directive covers the processing of personal data captured through a video surveillance system. Specifically, the Directive includes the recording, transmission, conservation or storage of images or audio for security, employee surveillance or other purposes.

3. What cases are not covered within the scope of this Directive?

There are four (4) scenarios:

- When one of the circumstances defined in Article 3 of the PDPL occurs. This article establishes which cases are not covered by the PDPL.[2]
- Processing of images captured on private property and images captured by video door-phone systems and devices.[3]
- Processing of images in the legitimate exercise of the right to the freedom of information and expression in the media.
- Systems which involve mock or inactive video cameras.

4. In which cases processing of personal data through video surveillance systems is legitimate?

There are three (3) scenarios:

- When the personal data subject consents to treatment of data.
- When a legal norm allows for data collection without consent.

---

1 Directive No. 01-2020-JUS/DGTAIPD.

2 For example, PDLP's article 3 establishes that personal data "*contained or destined to be contained in databases of the public administration*" is outside the scope, as long as it is required for the development of the functions of the administration, according to its competence recognized by law.

3 It should also be noted that the systems of video door-phone devices that have certain characteristics could be found within the scope of the Directive.

- When one of the circumstances defined in the Article 14 of PDPL occurs. This article establishes cases which do not require the consent of the personal data holder for the treatment of data.[4]

5. What is the maximum time frame allowed for the storage and destruction of data?

Images and audio can be stored for a maximum of sixty (60) working days, unless otherwise stipulated in the sectorial regulation rules. Following the expiration of the given period, and as a rule, the data shall be destroyed within a period of not more than two (2) working days.

6. What are the principal obligations established by the Directive?

- Any person who uses video surveillance systems for the purposes provided by the Directive shall register the database with the governmental agency, the Peruvian Personal Data Protection Authority.[5]
- The ability to monitor through video surveillance systems may only be carried out when pertinent, adequate and not excessive for its purposes. [6]
- The recording of third persons that may appear in the scene should be avoided, in accordance to the protection of their fundamental rights. This prevents the recording of public spaces, unless the surveillance requires that a specific area be recorded, in which case, the area covered by the camera must be limited to the aforementioned purposes.
- At the surveilled areas, there should be at least one distinctive poster in a sufficiently visible place informing that images are being captured and/or recorded. This poster should follow the design as outlined in the Appendix of the Directive.[7]
- The personal data holders' rights to access, cancellation and opposition must be guaranteed.
- Diverse security measures should be implemented to protect the information and to limit access only to personnel specifically appointed to manage the video surveillance system (for example, implement profiles, distinguish user privileges, etc.).
- When the management of the video surveillance system is entrusted to a third party, an agreement must be subscribed with the person responsible for establishing the objective, duration, and other relevant aspects of the services. Likewise, the database holder or the person responsible for managing the database should sign a confidentiality agreement with the third party designated to operate or access the video surveillance system.

7. Are there specific provisions for certain sectors?

Yes. For example:

- Video surveillance systems at financial entities shall exclusively be used for security purposes only. Images that record alleged commission of offenses must be immediately sent to the National Police of Perú or the Public Ministry.
- Surveilled areas at educational institutions must be kept to the minimum required, although common spaces such as accesses, corridors, courtyards and dining areas may be covered. Video surveillance systems in classrooms and similar environments will only be allowed to record images under exceptional circumstances, justified by foreseeable risks to security and minors' rights. Access to the images is furthermore restricted to the principal of the educational institution or the person designated as responsible for that function. Images can be stored for a maximum of thirty (30) working days.

---

4 For example, the article 14 of PDPL establishes that consent will not be required "*when the personal data is necessary for development of a contractual relationship where the personal data subject is a party*".

5 It must be pointed out that systems that do not store images (for example, systems that process real-time images) do not constitute a database.

6 If the surveilled area covers multiple areas, the poster should be placed in all of them.

7 As the poster indicates, it should be noted that all the information required by Article 18 of the PDPL (purposes for which the personal data will be processed, who will be or who may be the recipient, the identity and the address of the controller of the database and others) must be supplied on a sheet.

- From a labor perspective, there is an exception to the rule of informed consent because, in accordance to the employer's management prerogatives, employers have the legal powers to conduct regular checks or implement measures to monitor the work activities of employees. This includes the collection or processing of personal data through video surveillance systems.

  Furthermore, unedited images and/or audio that reveal the commission of alleged labor offenses and/or occupational accidents can only be stored for a maximum period of one hundred and twenty (120) days counted from the date of knowledge of the alleged offense, unless a legitimate interest or any justified purpose to prolong the conservation of the data were to exist. It is understood that this period allows the employer to take the appropriate legal actions and the recording may be used as evidence to support the employer's position, however, a copy must be given to the employee.

- The Directive also defines the treatment of personal data through other technologies. In the case of webcams, the database holder should ensure that the functions of identification and authentication are activated in the system to protect the information against the third-party access. Persons designated in charge of using video surveillance drones must be qualified to handle the equipment and follow the provisions of the Directive.

8. When will this Directive take effect?

The Directive will come into force in sixty (60) calendar days following its publication.

* * *

For any clarification or additional information regarding the content of this memorandum, please contact Mr. Carlos Patrón, Mr. Giancarlo Baella, Ms. Ana Lucia Figueroa or Ms. Jimena Pérez at +511-612-3202. To obtain a copy of the aforementioned regulation, please contact Mr. Paul Manrique at: **pmb@prcp.com.pe**