apdcat
Autoritat Catalana de Protecció de Dades

Opinion in relation to the query made by the data protection representative of an entity regarding the possibility of providing the identification data of surveillance personnel to users

A request is submitted to the Catalan Data Protection Authority for an opinion from the data protection officer (DPD) of an entity regarding the possibility of providing the identification data of surveillance personnel to users.

In the consultation, it is stated that the entity outsources the surveillance service of its stations, trains and facilities to different security companies that operate in the market and that these companies have contracted security guards who have the their title and qualification to carry out the functions entrusted to them.

As indicated, on occasion, there are users who do not agree with the way a security guard acts and present the corresponding claim to the entity's customer service, requesting the identification data of the specific security guard (name, surname, TIP) for the purposes of taking legal action against him.

In accordance with these antecedents, the DPD requests a statement regarding the following issues

"a) It would be lawful data processing to provide the identification data of the security guard, who provides service in the facilities of (...) and is contracted by a third company, to the user who has presented a claim to the customer service of (...), without having obtained the prior and express consent of the affected security guard?

b) What would be the legality of the treatment provided for in article 6 of the RGPD?
In particular, what would be the cause of legality other than the explicit consent that the interested person (security guard) could give?

c) If so, what would be the personal data that could be provided (name and surname, TIP)?

d) If they can be provided, it would be necessary for (...) to inform the affected security guard and/or the security company that has contracted him that his data has been requested by a user person at the root of a claim received and have they been provided to this user person?"

Having analyzed the query, which is not accompanied by other documentation, in accordance with the report of the Legal Counsel, I issue the following opinion:

I

(...)

II

The issues raised by the data protection officer are related to the communication of identifying data (name, surname and TIP) of the security guards of
trains, stations and other facilities of the entity, when they are required by users of the service who have submitted a claim to the entity's customer service.

As indicated in the query, these security guards are staff hired by the security companies that provide their services to the entity.

In this context, the first question that arises is whether to provide the identification data of the security guard, who provides service in the entity's facilities and is contracted by a third company, to the user who has submitted a claim to customer service of the entity, without having obtained the prior and express consent of the security guard concerned, would be lawful treatment.

The applicant for this opinion is a public law entity, with its own and independent legal personality that acts as a commercial company and is governed in accordance with the provisions of article 5 of its statutes, *"for these statutes, by Law 4/1985, of March 29, of the Statute of the Catalan Public Company, by the rules of civil, commercial and labor law, by the sectoral regulations governing land transport and, throughout the that is applicable, by Legislative Decree 9/1994, of July 13, which approves the revised text of the Public Finances Law of Catalonia, by Law 11/1981, of December 7, on heritage, as well as for the rest of the applicable provisions, especially those relating to the exercise of administrative powers and guardianship relations with the public administration".*

According to the information provided and the contractual documentation published in your contractor profile, the surveillance service of the entity's trains, stations and premises is provided through external security companies.
As stated in the special administrative clauses of the contract *"Security and surveillance service, dependencies and mobile equipment of the Metropolitan Lines and Lleida La Pobla de Segur Line (...)" (currently* in tender):

> *"The successful tenderer will be responsible for the work carried out by the people who are responsible for carrying out the provision and will notify (...) all the personnel who will provide services and carry out the works in their dependencies, and the variations that occur .*

Therefore, the information about the security guards who provide services in the branches and rolling stock of the railway lines is information held by the entity
as a result of the execution of the service contract between that and the security companies awarded the contract.

The consultation is focused on these terms, in order to answer the questions raised
by the DPD it is necessary to take into account that Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereinafter,

RGPD)), establishes that all processing of personal data, understood as *"any operation or set of operations carried out on personal data or sets of personal data, whether by automated procedures or not, such as collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of enabling access, comparison or interconnection, limitation, suppression or destruction" (article* 4.2 RGPD) must be legal, fair and transparent in relationship with the interested *party (article 5.1.a)).*

In order for a treatment to be lawful, it is necessary to have, at least, a legal basis of those provided for in article 6.1 of the RGPD, which establishes:

"a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures;

c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment;

d) the treatment is necessary to protect the vital interests of the interested party or another natural person;

e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment;

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child.

(...)"

As can be seen from article 6.3 of the RGPD and expressly included in article 8 of the LOPDGDD, data processing can only be considered based on the bases legal provisions of article 6.1.c) and 6.1e) of the RGPD when so established by a rule with the rank of law.

At the same time, according to article 86 of the RGPD: *"The personal data of official documents in the possession of any public authority or public body or a private entity for the performance of a mission in the public interest may be communicated by said authority, body or entity in accordance with the Law of the Union or of the Member States that applies to them in order to reconcile public access to official documents with the right to the protection of personal data under this Regulation."*

Given this, mention should be made of Law 19/2014, of December 29, on transparency, access to public information and good governance (LTC), which aims, among others, to *"regulate and guarantee the right of people's access to public information and documentation" (article* 1.1.b)).
This law and the regulation that develops it are applicable to the entity in accordance with the provisions of article 3.1.b) LTC.

Article 18 of the LTC establishes that *"people have the right to access public information, referred to in article 2.b, in an individual capacity or in the name and representation of any legally constituted legal person" (section* 1).

According to article 2.b) of the LTC it is *"public information: the information prepared by the Administration and that which it has in its possession as a result of its activity or the exercise of its functions, including that supplied by the other obliged subjects in accordance with the provisions of this law."*

In the case raised in the consultation, the identification data (name, surname, TIP) of the security guards of the trains, stations and other departments of the railway lines it is information that is in the entity's possession as a result of the execution of the contract for the provision of security services. This information must be considered public information for the purposes of the LTC which remains subject to the access regime provided for in this regulation, which establishes, as a general criterion, that the right of access to public information can only be denied or restricted for the reasons expressly established by law (article 20 et seq.).

Therefore, the provisions of the LTC in relation to articles 6.1.e) and 6.1.c) of the RGPD could constitute a legal basis for the communication, by the entity, of information about the security guards who provide services in its dependencies when they are requested by a user of the transport service.

However, to the extent that it is information that contains personal data, they may result apply the limits provided for in articles 23 and 24 of the LTC.

III

In cases where the information does not contain special categories of data in terms of Article 23 LTC, as would be the case of the information referred to in the query, access must be governed by the provisions of article 24 of the LTC, according to which:

"1. Access to public information must be given if it is information directly related to the organization, operation or public activity of the Administration that contains merely identifying personal data unless, exceptionally, in the specific case it has to prevail over the protection of personal data or other constitutionally protected rights.

2. If it is other information that contains personal data not included in article 23, access to the information can be given, with the previous reasoned weighting of the public interest in the disclosure and the rights of the people affected. To carry out this weighting, the following circumstances must be taken into account, among others:

a) The elapsed time.
b) The purpose of access, especially if it has a historical, statistical purpose or scientific, and the guarantees offered.
c) The fact that it is data relating to minors.

d) The fact that it may affect the safety of people.
(...).”

According to article 24.1 of LTC, access must be given to information directly related to the organization, operation or public activity of the administration that contains merely identifying personal data.

The merely identifying data of the security guards who provide services to the trains, stations and other dependencies of the entity, must be considered included within the provisions of article 24.1 LTC. These workers, despite not having an employment relationship with the entity, given the specific functions they carry out, directly related to the public functions of the entity, should be able to be identified by the users of the service in the same way as public employees would be who provide services in public administrations.

Thus, in the case raised in the consultation, if the information requested by a user of the entity's service for the presentation of a claim is only the identification data of a security guard, it would be necessary to provide him with the 'access to this information in accordance with article 24.1 LTC except that, in the specific case, the protection of the personal data of the supervisor involved should prevail.

Apart from this there is still another additional element that can lead to the same conclusion. From the perspective of data protection, it should be noted that, according to the tenth additional provision of the LOPDGDD:

"The responsible persons listed in article 77.1 of this organic law may communicate the personal data requested by subjects of private law when they have the consent of the affected or appreciate that the applicants have a legitimate interest that prevails over the rights and interests of those affected in accordance with the provisions of article 6.1 f) of Regulation (EU) 2016/679".

The legal basis of article 6.1.f) RGPD does not apply when data processing is carried out for the fulfillment of a mission carried out in the public interest or in the exercise of public powers of the person in charge. However, the tenth additional provision of the LOPDGDD provides for an authorization for communication based on the legitimate interest of third parties, as it could be, in this case, the affected users who request access to the data of a security guard safety

In the context raised in the consultation we can understand that the purpose of the access would be related to the defense of the interests of the person requesting since in order to undertake legal actions for the defense of their interests, the users of the service who have complaints about the treatment received by a security guard must be able to access certain information about them.

In accordance with what has been presented so far, the answer to the first and second of the questions raised by the DPD is that the communication of the merely identifying data of the security guard to a user who requests it for to submit a claim, it can be considered a lawful treatment that has as a legal basis the provisions of the LTC in relation to article 6.1.c) RGPD (the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for treatment).

IV

With regard to the personal data that can be communicated by the security guards, and in order to answer the third of the questions raised, it is necessary to attend to what is established in the transparency regulations.

Sections 2 and 3 of article 70 of Decree 8/2021, of February 9, on transparency and the right of access to public information (hereafter RLTC), provide.

"(..)
2. For the purposes of what is provided for in article 24.1 of Law 19/2014, of December 29, personal data consisting of the name and surname, the position or position held, body and scale, the functions performed and the telephone number and addresses, postal and electronic, of professional contact, referring to personnel in the service of public administrations, senior officials and managerial staff in the public sector of public administrations.

In cases where the publication or access to an administrative document requires the identification of the author, the location data, the number of the national identity document or equivalent document must be removed in particular and the handwritten signature. If the signature is electronic, the electronically signed document must be published in such a way that the properties of the electronic certificate used for the signature cannot be accessed.

The location data must be deleted in the event that it is not merely identifying data of the author in his position or staff in the service of the public administrations.

3. In the case of members of the forces and security forces or other groups that for security reasons require special protection, their identification with names and surnames must be replaced by the publication of a code or professional identification number.

(...)"

Thus, in the case of security forces and bodies, but also of other groups that for security reasons require special protection, the identification with names and surnames must be replaced by the communication of a professional identification number .

In the case of security guards, they must be in the regime established by Law 5/2014, of April 4, on Private Security.

According to article 2.1 of this law, private security is *"the set of activities, services, functions and security measures adopted, voluntarily or mandatory, by natural or legal persons, public or private, carried out or provided by security companies, private detective agencies and private security personnel to deal with deliberate acts or accidental risks, or to carry out investigations on people and goods, with the aim of guaranteeing the safety of people, protecting their heritage and safeguarding for the normal development of their activities".* While article 2.8

defines private security personnel as: *"the physical persons who, having obtained the corresponding qualification, develop private security functions".*

The qualification requirements for security guards are regulated in article 27 which establishes:

"1. For the exercise of private security functions, the staff referred to in the previous article must previously obtain the corresponding qualification from the Ministry of the Interior, in the terms that are determined by regulation.

2. To those who apply for the qualification, after checking that they meet the necessary requirements, they will be issued the professional identity card, which will include all the qualifications that the holder has.

The professional identity card will constitute the public document of accreditation of the private security personnel while they are in the exercise of their professional functions.

(...)"

Article 39.5 provides that the security personnel during the provision of their services must carry the professional identification card.

In the same sense, Royal Decree 2364/1994, December 9, which approves the Private Security Regulation, also establishes in its articles 52, 60 and 68 the qualification of this staff and the documentation of this qualification through the corresponding card of professional identity, as well as the obligations to carry the personal identification card as long as they are in the exercise of their functions and to show them when required by members of the bodies and security forces or by the affected citizens (article 68.2).

Therefore, to the extent that the analyzed private security regulations foresee an identification of these through a professional identity card (TIP) it must be understood that they are being recognized by the special protection referred to in the article 70.3 of the RLTC.

Consequently, the identification data of security guards that can be provided to people who request it to make a claim, must be limited to the TIP of the guards without including their first and last names.

V

Finally, the DPD considers whether it is necessary for the entity to notify the affected security guard and/or the security company that has contracted him of the fact that his data has been requested, by a root user of 'a claim received and provided to this user.

With regard to this issue, article 31 of the LTC should be taken into consideration, which provides for the following:

"1. If the request for public information may affect the rights or interests of third parties, in accordance with the provisions of this law, in the event that the potential affected are identified

or are easily identifiable, they must be forwarded the request, and they have a period of ten days to present allegations if these may be decisive for the meaning of the resolution.

2. The claims procedure referred to in section 1 suspends the deadline for resolution.

3. The transfer of the request must indicate the reasons for the request, if they have been expressed, but it is not mandatory to reveal the identity of the applicant.

4. The applicant must be informed of the transfer of the application to third parties and of the suspension of the deadline for issuing a resolution until the allegations have been received or the deadline for presenting them."

Thus, in order to be able to determine whether there are personal circumstances affecting the security guard whose data is requested that, exceptionally, could limit this right of access, it would be necessary to notify the security guards affected of the fact that their data have been requested by a user, before providing it to him
person their data, so that they can make the allegations they consider appropriate.

Regarding the communication of this request to the security company, this is a matter that is not provided for in the data protection regulations and is therefore not the subject of this opinion.

In any case, in the communication to the affected person derived from article 31 LTC, it must be taken into account that in principle the identity of the person claiming must not be included (art.
31.3 LTC and 62.4 of the RLTC), unless exceptionally, in a motivated manner and after consultation with the applicant, he considers that communicating his identity may be essential for the defense of the rights and interests of the private security guard.

On the other hand, article 34.1 of the LTC establishes that the resolution of the access request, apart from being notified to the applicant, must also be notified to the affected persons - in in this case the security guard - who have appeared in the file.

In short, from the point of view of data protection regulations, the entity should notify the affected security guard that their data has been requested by a user before providing them with their information in such a way that this one can
allege the personal circumstances it deems appropriate and, where appropriate, exercise the right of opposition provided for in article 21 of the RGPD.

conclusion

The entity making the inquiry can communicate the TIP number, without including the first and last names, of the security guards who have intervened in any incident during the provision of the service, at the request of any user who has participated in the events .
This communication would find qualification in article 6.1.c) RGPD in relation to the LTC.

The entity should notify the affected security guard that their data has been requested by a user before providing them with the information so that, if applicable,

can allege the personal circumstances on which he bases his opposition to access. Once the resolution of the access request has been issued, the security guard or guards who have appeared in the file must also be notified.

Barcelona, June 3, 2022