Machine Translated by Google

apdcat
Autoritat Catalana de Protecció de Dades

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

File identification

Sanctioning procedure no. PS 8/2018, referring to the General Directorate of Penitentiary Services of the Department of Justice

Background

1. On 22/08/2017 the Catalan Data Protection Authority received a letter from a trade union for which it filed a complaint against the Directorate General of Penitentiary Services of the Department of Justice (hereinafter, DGSP), with due to an alleged breach of Organic Law 15/1999, of December 13, on the protection of personal data (hereinafter, LOPD). Specifically, the reporting entity stated that the user code to access the information systems of the penitentiary centers (and in particular, the Barcelona Women's Penitentiary Center - henceforth, CP Women -) coincided with the DNI of the employees, which could be visible to internal people while logging into the corresponding terminal. The reporting entity added that the printing of documents contained the ID of the person who had done it; as well as that on a certain screen of the operating system the user's name and surname were also displayed.

   The reporting entity provided various documentation relating to the events reported.

2. The Authority opened a preliminary information phase (no. IP 226/2017), in accordance with article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (hereinafter, LPAC), in order to determine whether the facts were susceptible of motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances concurrent in each.

3. As part of this information phase, on 22/11/2017 the Authority carried out an inspection at the CP de Dones, in order to verify certain aspects related to the identification of people users of the information systems of the penitentiary center. In that face-to-face inspection, the representatives of the inspected entity stated, among others, the following:

   - That the code to access the corporate information systems of the penitentiary centers is the employee's ID since 2015.
   - That no other identification code is used for the user, such as the personal identification number (hereafter, NIP), because the information systems are corporate (of the Generalitat de Catalunya) and do not depend on the Department of Justice.

Machine Translated

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- That the inmates cannot view the screen of the computer equipment of the employees of the penitentiary center.

ÿ That when a print is made, the sheets contain a SIPC user code, which does not match the DNI.

Likewise, the Authority's inspection staff verified, among others, the following:

ÿ That at the desk where an official provides services, adjacent to the entrance door to the penitentiary staff cafeteria, there was a computer equipment. In this sense, the representatives of the inspected entity stated that the internal access door to the interior of the penitentiary (located next to the official's desk) was not accessible to inmates. The inspection staff made a photographic report of this dependence and the location of the terminal screen.

- That when the computer is locked, no personal data of the user was shown on the screen. In turn, it was found that the user code to start the computer session corresponded with the ID of the user. Once it started, there was no personal data on the desktop screen. On the other hand, if accessed in the "Start" menu (which does not correspond to the desktop), the first and last names of the public employee were written in the upper right part. A photograph was taken of each of the checks mentioned in this section.

The representatives of the inspected entity delivered a copy of the parametric list of diets, at the request of the inspecting staff. In the heading there was a numerical user code, which did not match the ID of the user who had carried out the printing, but the user number (6 digits).

4. On 04/03/2018, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against the DGSP, as an alternative, for an alleged serious infringement provided for in article 44.3.c) in relation to article 4 LOPD; or, for an alleged serious infringement provided for in article 44.3.d) in relation to article 10 LOPD. Likewise, he appointed the official of the Catalan Data Protection Authority, (...) as an instructor of the file. This initiation agreement was notified to the imputed entity on 04/04/2018.

In the initiation agreement itself, the reasons why no imputation was made regarding the fact reported relating to the inclusion in the DNI documents of the user who carries out the printing, given that in the act of in-person inspection carried out on 22/11/2017, the Authority's inspector staff verified that the printed document did not contain this data, but rather its SIPC user code (of 6 digits) corresponding to the prison information systems .

Machine Translated

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

5. The Department of Justice made objections to the initiation agreement by means of a letter dated 04/20/2018, in which it stated that it was not competent to define the policy of access to corporate information resources.

6. By Agreement dated 05/10/2018, the instructor ordered the opening of a test period, in order to practice the test consisting of requiring a report to the Department's Department of Telecommunications, Cybersecurity and Digital Society of the Presidency on whether the Department of Justice can decide how to set up the code through which the users of the information systems of the penitentiary centers are identified (currently, it is the DNI of the user) to start the session in the operating system; or if, on the contrary, the decision on the configuration of the user code corresponds to another body (such as the Secretariat itself) or body. This Agreement was notified to the Secretariat of Telecommunications, Cybersecurity and Digital Society and the Department of Justice on 05/10/2018.

The Telecommunications and Information Technologies Center of the Generalitat de Catalunya (hereinafter, CTTI) issued the required report on 05/24/2018. In this report, among others, the CTTI stated the following:

ÿ That in 2014 the CTTI carried out an analysis of the different ways in which public employees identified themselves with the IT resources of the Generalitat de Catalunya (workstation, information systems, etc.).
- As a result of this analysis, it was found not only the diversity of existing forms of identification, but that the same user used different forms of identification to access the IT resources he needed to perform his function.

ÿ That in the face of this situation, the CTTI proposed to homogenize as much as possible the way in which a user could identify himself, and after analyzing different options, the NIF was considered as a universal and simple identifier for all public employees to remember, and so it was proposed to Public Function to obtain its approval.

ÿ That in this same proposal it was indicated that the NIF be used in a generalized way, except for those collectives of the Generalitat of Catalonia that, due to their uniqueness, require a different code, as for example the case of
little ones
- With respect to the specific case of the Penal Execution collective, two cases must be considered:

1. Access to the workstation. During the process of transforming this collective's workstation, at the "kickoff" of the project, information was given on the general proposal to deploy the NIF as an authentication code, and it was accepted by Department of Justice, although the NIF was requested to be hidden on the screens where it appeared. It was agreed to carry out the

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

transformation and plan this task as an activity to be performed at the end of the deployment. At the moment the task is being planned.

If the option to be carried out does not consist of "hiding the NIF", but of changing the authentication code, the CTTI considers that it is viable but that it would be neither trivial nor transparent for the user, since all the services in which is accessed from the workstation (print service, file service, email service, etc...) are currently linked to this NIF user code.

2. Access to Criminal Enforcement applications (SIPC). The information contained in the CTTI is that the SIPC application is not integrated with the corporate identity management system, GICAR, and therefore the user and password synchronization mechanisms are not applied to it, nor is it under the process GICAR user authentication. In any case, it should be noted that GICAR allows, apart from the NIF -primary identifier-, the use of a second identifier.

ÿ That it is up to the Department of Justice to establish the requirements it considers necessary for the identification of its staff, raising the exceptions to the general rule it considers necessary to the CTTI so that they are implemented by the Workplace provider.

7. On 07/30/2018, the person instructing this procedure formulated a proposed resolution, which proposed that the director of the Catalan Data Protection Authority declare that the DGSP had committed a serious infringement, provided for in article 44.3.c), in relation to article 4, both of the LOPD.

8. This resolution proposal was notified on 07/31/2018 and granted a period of 10 days to formulate allegations. The deadline has been exceeded and no objections have been submitted.

Machine Translated

proven facts

Of all the actions taken in this procedure, the facts detailed below are considered accredited.

For security reasons, the staff who provide services in penitentiary centers are identified in their professional activities, through the professional identity card number (hereafter, TIP).

The users of the information systems of the penitentiary centers are identified through their DNI to access said systems (authentication is through passwords). This code, which differs from the TIP given to prison staff for security reasons, is visible for the duration of the authentication process when starting or restarting the computer session.

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

In turn, once the computer session has started on the terminal, when the "Start" menu of the operating system is accessed, the user's first and last name is displayed.

Therefore, identification data (DNI and first and last name) are used that are different from the identification data that the Directorate General of Penitentiary Services of the Department of Justice gives to prison officials so that it can be used in their professional actions, for reasons of security.

Fundamentals of law

1. The provisions of Law 39/2015, of October 1, on the common administrative procedure of public administrations (from now on, LPAC), and article 15 of Decree 278 apply to this procedure /1993, of November 9, on the sanctioning procedure for application to the areas of competence of the Generalitat, according to what is provided for in DT 2a of Law 32/2010, of October 1, of the Catalan Authority of Data Protection. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

   As a preliminary consideration, it should be indicated that at the time this act was issued, the precept containing the infringing rate applied here has been repealed by Royal Decree-Law 5/2018, of 27/7, on urgent measures for the adaptation of Spanish law to the regulations of the European Union in the matter of data protection. But since it is a sanctioning procedure started before the validity of this rule - or in which the previous actions that had preceded it had started before -, it must be governed by the previous regulation (DT 1a RDL 5/2018).

   Also, in this act, the eventual application to the present case of what is provided for in Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, regarding the protection of natural persons, has also been taken into account regarding the processing of personal data and the free movement thereof (RGPD). And as a result of this analysis, it is concluded that the eventual application of the RGPD would not alter the legal classification that is made here, and in particular would not favor the presumed person responsible for the infringement. In any case, it is worth saying that the facts imputed in application of the LOPD would also be so if the RGPD were applied to the case, in accordance with the provisions of article 83.5.a) RGPD in relation to the article 5.1.e) RGPD

2. The accused entity has not made allegations in the resolution proposal, but it did so in the initiation agreement. Regarding this, it is considered appropriate to reiterate below the most relevant part of the motivated response of the instructing person to these allegations.

Machine Translated

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Well, in the statement of objections presented before the initiation agreement, the Department of Justice considered that it was not competent to define the policy of access to information resources.

As the instructing person pointed out, in the present case the Department of Justice is responsible for the treatment subject to imputation, given that it is the one who decides on: "the purpose, content and use of the treatment" (art. 3. d of the LOPD).

Specifically, as indicated by the CTTI in the report issued in the evidentiary phase, it is up to the Department of Justice to establish the necessary requirements for the identification of its personnel. In this sense, the CTTI indicated that within the framework of the transformation program initiated in 2014 to homogenize the identification of the staff of the Generalitat de Catalunya with regard to computer resources, in general, the NIF was considered as a universal identifier (except for those collectives of the Generalitat de Catalunya that, due to their uniqueness, require a different code, such as the case of the police). For the specific case of the Department of Justice, the CTTI stated that at the beginning of the project it accepted the use of the NIF as an identification element for its staff to access the workstations.

Regarding the DNI as an identifying element of the users assigned to the penitentiary center in the information systems, Order JUS/177/2004, of May 27, which approves the TIP model for the staff assigned to the units and centers that depend on the Secretariat of Penitentiary Services, Rehabilitation and Juvenile Justice, determines that penitentiary services staff must not be identified through their first and last names or ID, but through the TIP of the staff of penitentiary services. So, we would be dealing with a unique group (the staff assigned to the penitentiary centers), comparable to the agents of the Police of the Generalitat-Mossos d'Esquadra, in relation to whom a identification mechanism different from that of the rest of the staff of the Generalitat de Catalunya.

Therefore, the NIF is considered inadequate and not relevant data to identify the users attached to the penitentiary centers in the information systems. Although the process of homogenization in the identification of users predates the application of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, relating to the protection of natural persons by regarding the processing of personal data and the free movement thereof (RGPD) - dated 05/25/2018 -, it is considered appropriate to highlight that this rule provides for data protection by design as one of the obligations that must contemplate both the person in charge and the person in charge of the treatment (art. 25 RGPD).

On the other hand, the CTTI admitted that the Department of Justice requested that the NIF be hidden on the screens where this data appeared, a task that was still being planned at the time of the report's issuance, although the homogenization of identification systems would have started in 2014.

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Without prejudice to what has been stated regarding the consideration of the DNI as a non-pertinent or adequate piece of data for the identification of users attached to penitentiary centers, it is not known that this request was formalized as an instruction from the Department of Justice to CTTI. And in any case, it is clear that the Department of Justice would not have ensured that, in relation to the personnel who provide services in the penitentiary centers, the identification was carried out in that way.

Aside from the above, although the imputed entity did not make allegations regarding the facts that were imputed in the initiation agreement and that are collected in the section on proven facts, relating to the fact that the name and surnames of the user is visible on the "Start" screen of the operating system, it must be noted that this data processing is also considered to be inappropriate, irrelevant and excessive, with the understanding that people who provide services in penitentiary centers, as advanced, they must be identified by their TIP for security reasons.

3. In relation to the facts described in the proven facts section, as indicated by the instructing person in the resolution proposal, it is considered that of the two legal qualifications that were made in the agreement to initiate the procedure penalty, with an alternative character, the application of the serious infringer type provided for in article 44.3.c) in relation to article 4 of the LOPD is more adjusted to the present case. In this regard, it is considered that Order JUS/177/2004 establishes that the staff attached to the penitentiary centers must be identified through the TIP of the penitentiary services staff. This is why it is considered that the use of the DNI as an identifying element that is visible during the authentication process of the computer session; as well as the processing of the user's name and surname on the "Start" screen of the operating system are inadequate, irrelevant and excessive data processing.

So, in relation to the facts described in the proven facts section, it is necessary to go to article 4.1 of the LOPD, which regulates the principle of data quality in its aspect of the principle of proportionality or minimization of the data, in the following terms:

> "1. Personal data can only be collected to be processed, as well as subjected to this processing, when they are adequate, relevant and not excessive in relation to the scope and the determined, explicit and legitimate purposes for which they are have obtained."

As indicated by the instructing person, during the processing of this procedure the fact described in the section on proven facts, which is considered constitutive of the serious infringement provided for in article 44.3.c) of the LOPD, which typifies as such:

> "c) Treat personal data or use them subsequently in compliance with the principles and guarantees established in article 4 of this

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Law and the provisions that deploy it, except when it constitutes a very serious infraction."

Apart from the above, articles 2 and 3 of Order JUS/177/2004 provide the following:

"Article 2

The professional identity card

The professional identity card accredits the status of staff in the service of the Generalitat in the sectoral scope of the Secretariat of Penitentiary Services, Rehabilitation and Juvenile Justice.

Article 3

The use of the professional identity card

3.1 The professional identity card is a personal and non-transferable element of identification. It is also a time control instrument.

3.2 The personnel addressed by this Order must use their professional identity number in all their professional actions, give this identity number when required by citizens in their professional actions, and display the card when they have to intervene as experts or witnesses in judicial proceedings, due to or as a consequence of their professional actions."

4. Article 21 of Law 32/2010, in line with article 46 of the LOPD, provides that when the infractions are committed by a public administration, the resolution declaring the commission of an infraction must establish the measures to be taken so that the effects cease or are corrected. By virtue of this faculty, as proposed by the instructing person, the Department of Justice should be required so that as soon as possible, and at the latest within 3 months from the day following the notification of this resolution, carry out the necessary actions so that the NIF of the staff assigned to the penitentiary centers is not used to identify themselves in the information systems; as well as so that it is removed from the "Start" menu of the operating system, the user's name and surname are displayed.

Once the corrective measure described has been adopted within the period indicated for the purpose, within the following 10 days the Department of Justice must report to the Authority, without prejudice to the inspection faculty of this Authority in order to carry out the corresponding checks.

resolution

For all this, I resolve:

Machine Translated

Machine Translated by Google

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

1. Declare that the General Directorate of Penitentiary Services of the Department of Justice has committed a serious infraction provided for in article 44.3.c) in relation to article 4, both of the LOPD.

2. Require the DGSP to adopt the corrective measures indicated in the 4th legal basis and certify to this Authority the actions taken to comply with them.

3. Notify this resolution to the DGSP.

4. Order that this resolution be published on the Authority's website (www.apd.cat), from in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with what they provide
article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

Machine Translated

The director

M. Àngels Barbarà and Fondevila

Barcelona, (on the date of the electronic signature)