Machine Translated by Google

apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 14/2020, referring to the Parc Taulí Health Corporation.

Background

1. On 17/05/2019, the Catalan Data Protection Authority received, by referral from the Antifraud Office of Catalonia, a letter indicating that more than "3,000 computers could be accessed of tabletops [which] are used at the Parc Taulí de Sabadell University Hospital", through the same user code ("CSPT") and password ((...)).

2. The Authority opened a preliminary information phase (no. IP 153/2019), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application 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 (henceforth, LPAC), to determine whether the facts they were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

3. In this information phase, on 07/09/2019, the Authority carried out an inspection at the premises of the Sabadell Hospital of the Parc Taulí Health Corporation (hereinafter, CSPT) , to verify certain aspects related to the facts. In that face-to-face inspection, the representatives of the CSPT stated the following:

- That CSPT employees, to start the computer session through the desktop computers, had to identify themselves through a user code and authenticate themselves through a password.

- That there were users who shared a user code and password. These generic user codes were used to access local drives on computers. To access personal data (folders, applications, network drives, etc.), each person had their personal user code.

- That the generic user codes were "CSPT", "consultations", "nursing" and "UDIAT".
- That in principle, no personal data was stored on the local hard drive of this computer. The users had network units that were personal and also group (for each unit), to store files with personal data.
- That in the corporate confidentiality guide, it was indicated generically that information with personal data could not be stored on local hard drives.
- That an action was taken so that, the users who justified it, could have more space in the personal and group network units.
ÿ That in order to access the applications used by the users (such as the one that allowed consulting the medical history), it was necessary to identify and authenticate again. The user code and password were different for each user.

Machine Translated by Google

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

- That a user and password were also available to access the network units staff
- That in approximately March 2019, the ability to access or connect to the hard drive of any other computer on the computer network was disabled.
- That it was planned to carry out a risk analysis to determine the appropriate technical and organizational measures to guarantee the security of the data processed by the CSPT through the IT network.

Also, on this same date, the Authority's inspection staff verified, among others, the following:

- That to start the computer session of the IT team of the visit programming unit, the user code was "CSPT" and the password was (...).
- That there were files in the "Documents" folder of the local drive of that computer that contained personal data, including health-related data.
ÿ That, to access the application to consult the patients' clinical history (HP-HCIS TAULI), the user code was personal.
- That to access the network units it was necessary to identify and authenticate beforehand. The user code was also personal.
- That the hard drive of another computer could not be accessed remotely.

4. On 02/06/2020, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against the CSPT for two alleged infringements, in both cases, provided for in article 83.4.a), in relation to article 32; all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free circulation thereof (hereafter, RGPD).

5. On 26/06/2020, the CSPT made objections to the initiation agreement.

6. On 09/15/2020, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority admonish the CSPT as responsible for two foreseen infringements in article 83.4.a) in relation to article 32, both of the RGPD.

This resolution proposal was notified on 09/25/2020.

7. On 08/10/2020, the accused entity submitted a letter in which it states that it does not make any objections to the proposed resolution, and simply reports on the actions taken to comply with the corrective measures that suggested the instructor.

In turn, the CSPT provided a copy of the risk analysis on the security of the workstations.

Machine Translated

Machine Translated by Google

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

proven facts

1. As informed by the representatives of the CSPT in the face-to-face inspection carried out on 07/09/2019 by the Authority's inspector staff, to start the computer session through the desktop computers, the users had to 'identify through a generic user code ("CSPT", "consults", "nursing" or "UDIAT") and authenticate using a password that was common to each generic user code.

As the Authority's inspector staff found in the same inspection act, once the computer session of the visit programming unit started with the user code "CSPT" and the password (...), documents with personal data relating to the health of CSPT patients were stored in the local unit of that team.

In turn, and as CSPT representatives admitted in the same inspection act, until approximately March 2019, once the computer session was started on the CSPT computer using a generic user code , it was possible to access or connect to the hard drive of any other computer on the computer network.

The Authority's inspector staff, verify in the inspection act that the hard drive of another computer could no longer be accessed remotely.

2. As the representatives of the CSPT also admitted in the inspection act, a risk analysis had not been carried out to determine the appropriate technical and organizational measures to guarantee the security of the data processed by the CSPT through of the computer network.

Fundamentals of law

1. The provisions of the LPAC, and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of the Catalan Data Protection Authority. 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.

2. As has been advanced in the antecedents, the CSPT has not formulated 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.

2.1. On the proven fact 1st.

Machine Translated

Machine Translated by Google

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

First of all, the accused entity pointed out in its statement of objections to the initiation agreement, that the provision of personal folders in network units (which require a password), ensured the possibility of 'store personal data with security measures in accordance with current regulations. And he added that the personal data shared in these folders was justified by the need for the attention given to the CSPT.

In relation to the above, as indicated by the instructing person in the proposed resolution, it is necessary to point out that neither of the two circumstances set out by the CSPT are subject to imputation in the present sanctioning procedure.

Secondly, the CSPT admitted that some users, as evidenced in the inspection carried out by the Authority's inspector staff, kept on the hard disk personal data that should be stored in the aforementioned network units. That is why the CSPT considered that this incidence should be limited to access to data on the local disk of computers without a personalized passkey.

Indeed, as set out in the 1st point of the proven facts section, the Authority's inspection staff found that once the information session had started, identifying with one of the generic user codes used by the CSPT, and by authenticating with a common password, it was possible to access documents with personal data relating to the health of CSPT patients that were kept in the local unit of a certain computer equipment.

On the contrary, as recorded in the 3rd precedent, in the act of on-site inspection the Authority's inspector staff verified that to access the application to consult the clinical history of the patients or the network units, the user code was personal.

And, thirdly, the CSPT argued that the audits carried out (the last one, in 2017) did not detect the incidents referred to in proven fact 1 of this proposal.

Well, the fact that the audits on data protection carried out by the CSPT did not detect the facts object of imputation, does not allow the CSPT to be exempted from responsibility.

2.2. About the corrective measures.

Subsequently, the accused entity alleged in its statement of objections to the initiation agreement that the deletion of generic users had been foreseen, but explained that the complexity of the project, the cost and the situation arising from the 'state of alarm, they had delayed it. However, the CSPT pointed out that it had resumed the project, which had been redefined in phases.

Machine Translated

Machine Translated by Google

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

While the said project is not being executed, and to ensure that no data can be stored without the need to authenticate, the CSPT stated that the space dedicated to user files had been expanded, which always required authentication through personal password.

Likewise, the CSPT indicated that through the intranet it had been communicated to all employees that files containing personal data could not be saved on the computer's hard disk, as it did not guarantee the security of the data; that information with personal data could not be saved outside the corporate databases (and that, if necessary, network folders should be used); as well as the storage space available to users had been expanded. With similar content, the CSPT sent a message to all employees via a pop-up window and set up another message that was displayed at the time of computer startup.

On the other hand, the CSPT also listed a series of measures that, in its judgment, evidenced its proactive responsibility (adherence to a certain type code, the performance of biennial audits, access by employees to the guide for the care of confidentiality, the dissemination of news on data protection through the intranet, the realization of monthly access registration audits, the realization of training activities on data protection, the appointment of a data protection delegate or the performance of different internal procedures).

In this regard, it is worth saying that the circumstances invoked by the CSPT to prove its proactive responsibility could be taken into account in order to graduate the financial amount of the penalty in the event that it consisted of the imposition of an administrative fine, of in accordance with what is established in article 83.4 of the RGPD.

However, in the present case the sanctioning regime applicable to the CSPT does not provide for the imposition of a financial penalty, but a warning in accordance with the provisions of article 77 of Organic Law 3/2018, of 5 December, of protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), which by its very nature is not susceptible to graduation.

At the very least, as the instructing person pointed out, it is appropriate to highlight and value the measures of proactive responsibility adopted by the accused entity and those it planned to implement following the events that are the subject of this sanctioning procedure, which must allow (when fully implemented) correct the effects of the infringement linked to the 1st proven fact (the use of generic user codes and passwords to start the computer session through the desktop computers, which allowed access to the computer's local drive in the which documents with personal data were stored, as well as the possibility of remotely accessing the hard drive of another computer in the CSPT network - which was amended during the month of March 2019, approximately-).

Machine Translated by Google

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

In the last one, the CSPT also detailed extensively a series of actions that were carried out to increase data security, as a result of the risk analysis report.

Well, in the proposed resolution the carrying out of said risk analysis by the CSPT was positively assessed (although this had not been provided).

Having said that, as explained by the instructing person, it is also necessary to point out that the adoption of measures to correct the effects of the infringement do not distort the imputed facts, nor do they modify their legal classification.

3. In relation to the two behaviors described in the proven facts section, it is necessary to go to article 5.1.f) of the RGPD, which regulates the principle of integrity and confidentiality determined that personal data will be "treated in such a way that an adequate security of personal data is guaranteed, including protection against unauthorized or illegal treatment and against accidental loss, destruction or damage, through the application of appropriate technical and organizational measures".

For its part, article 32.1 of the RGPD provides that "Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of probability and variable severity for the rights and freedoms of physical persons, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk (...)."

In turn, article 32.2 of the RGPD provides that "When evaluating the adequacy of the security level, particular consideration will be given to the risks presented by data processing, in particular as a consequence of accidental destruction, loss or alteration or illegal transfer of personal data, stored or otherwise processed, or unauthorized communication or access to said data."

This implies having to carry out an assessment of the risks involved in each treatment, in order to determine the security measures that need to be implemented.

Without prejudice to said assessment, paragraph 2 of additional provision 1a of the LOPDGDD establishes that "Those responsible listed in article 77.1 of this Organic Law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promoting a degree of implementation of equivalent measures in the companies or foundations subject to private law linked to them."

In this sense, article 16 of Royal Decree 3/2010, of January 8, which regulates the National Security Scheme (ENS) in the field of Electronic Administration, foresees as one of the minimum requirements of security regarding authorization and access control, that "Access to the information system must be controlled and limited to

Machine Translated

Machine Translated by Google

duly authorized users, processes, devices and other information systems, restricting access to the permitted functions."

In the present case, however, the use of a generic identification and authentication system to start the session on the computer equipment, did not guarantee access control.

As indicated by the instructing person, during the processing of this procedure they have duly accredited the two behaviors described in the proven facts section, which are constitutive of two infractions, both provided for in article 83.4.a) of the RGPD, which typifies the violation of "the obligations of the person in charge and of the person in charge pursuant to of articles 8, 11, 25 to 39, 42 and 43", among which there is that provided for in article 32 RGPD.

The conduct addressed here has been included as a serious infraction in article 73.f) of the LOPDGDD, in the following form:

> "f) The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679."

4. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, the competent data protection authority:

> "(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the conduct ceases or the effects of the offense committed are corrected.
>
> The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to those affected who have the status of interested party, if applicable."

In terms similar to the LOPDGDD, article 21.2 of Law 32/2010, determines the following:

> "2. In the case of violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects . In addition, it can propose, where appropriate, the initiation of disciplinary actions in accordance with what is established by current legislation on the disciplinary regime for personnel in the service of public administrations. This resolution must be notified to the person responsible for the file or the treatment, to the person in charge of the treatment, if applicable, to the body to which they depend and to the affected persons, if any".

Machine Translated

Machine Translated by Google

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

As has been advanced in the antecedents, by means of a letter of 08/10/2020 the CSPT has provided a copy of the risk analysis on the security of the workstations, which is why it is not appropriate to require any corrective measures in relation to the proven fact 2nd.

On the other hand, in relation to the corrective measure proposed by the instructing person in the resolution proposal regarding the 1st proven fact, the CSPT informs in its letter of 10/08/2020 that the corrective actions have been initiated opportune to respond within the deadline indicated in the resolution proposal, which must be assessed positively.

Given the above, the CSPT should be required to carry out the necessary actions as soon as possible, and in any case within a maximum period of 3 months from the day after the notification of this resolution, to guarantee the personalized identification and authentication of users authorized to access computer equipment; deleting the now existing generic users.

Once the corrective measure described has been adopted, within the specified period, the CSPT must inform the Authority within the following 10 days, without prejudice to the inspection powers of this Authority to carry out the corresponding checks.

resolution

For all this, I resolve:

1. Admonish the Parc Taulí Health Corporation as responsible for two violations provided for in article 83.4.a) in relation to article 32, both of the RGPD.

2. Require the CSPT to adopt the corrective measure indicated in the 4th legal basis and certify to this Authority the actions taken to comply with it.

3. Notify this resolution to the CSPT.

4. Communicate the resolution issued to the Grievance Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

5. Order that this resolution be published on the Authority's website (apdcat.gencat.cat), 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 file a contentious appeal directly

Machine Translated

Machine Translated by Google

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

administrative 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.

The director,

Machine Translated