apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 9/2020, referring to the Official College of Psychology of Catalonia.

Background

1. En data 29/03/2019 va tenir entrada a l'Autoritat Catalana de Protecció de Dades, per remissió de l'Agència Espanyola de Protecció de Dades, un escrit d'una persona pel qual formulava una denúncia contra el Col·legi Official of Psychology of Catalonia (hereinafter, COPC), due to an alleged breach of the regulations on personal data protection. Specifically, the person making the complaint indicated that he had been a user of the private area of the COPC website for more than 8 years, a period in which he had never had to change his password to access it.

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

2. The Authority opened a preliminary information phase (no. IP 101/2019), 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 04/12/2019 the reported entity was required to report, among others, on whether it had implemented a system for changing passwords for users of the private space of the school website at a given frequency.

4. On 04/29/2019, the COPC responded to the aforementioned request through a letter in which it stated, among others, the following:

- That the COPC implemented the password change system for users of the private space of the school website in September 2018, to mitigate the risks detected in the analysis.

- That the implementation of this measure was carried out as soon as possible, taking into account the availability of the necessary economic and technical resources to carry out the.

- That the periodicity planned for changing the password was one year.
- That the change could be voluntary, because the employee decided to change the password before the year; or it could be mandatory. After the year, the user had to change the password compulsorily.

- That if I didn't change it, every time I accessed the private space a message would pop up asking me to change the password. The notice of the change was not occasional, since it came out every time

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

access until the user changed the password. If he didn't, he couldn't make changes in his personal area.

The reported entity attached various documentation to the letter.

5. On 06/03/2020, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the COPC for an alleged infringement provided for in article 83.4.a), in relation to the 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 movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 03/11/2020.

6. On 03/23/2020, the COPC made objections to the initiation agreement.

The accused entity provided various documentation with its letter.

7. On 02/06/2020, the person instructing this procedure formulated a resolution proposal, for which he proposed that the director of the Catalan Data Protection Authority admonish the COPC as responsible for an infringement provided for in article 83.4.a) in relation to article 32; all of them from the RGPD.

This resolution proposal was notified on 06/17/2020 and a period of 10 days was granted to formulate allegations.

8. The deadline has been exceeded and no objections have been submitted.

proven facts

Until September 2018, the COPC had not implemented the security measure consisting of establishing the periodicity with which the passwords of the users of the private space of the school website had to be changed.

The COPC decided to start implementing this security measure on 09/19/2018, as a result of the risk analysis carried out.

Despite having passed the period of validity of the password provided by the COPC (1 year), the user of the private space of the college website could continue to access it without changing his password until 04/30/2019.

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, la

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

resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

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.

Well, the COPC explained in its statement of objections to the initiation agreement that by means of 04/26/2019 it already indicated the measures adopted to implement, from September 2018, the security measure consisting in establishing the periodicity with which the passwords of the users of the private space of the school website had to be changed. The COPC added that, following the response to the request made by the Authority, on 04/30/2019 the relevant actions were carried out in order to prevent the users of the private space of the web school could continue to access it without changing their password. These actions consisted of redirecting the navigation through the private space of the web to the screen to modify the password.

As stated by the instructing person in the resolution proposal, it must be made clear that the accused entity did not question the facts attributed to it in the initial agreement.

Having said that, 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 change their legal classification.

Given the above, it is appropriate to positively assess the actions of the COPC in order to guarantee the security of the data of the users of the private space of its website, effectively implementing the security measure consisting in establishing the periodicity with which passwords had to be changed.

3. In relation to the facts described in the proven facts section, it is necessary to refer to article 93.4 of Royal Decree 1720/2007, of December 21, which approves the Regulation for the implementation of Organic Law 15/ 1999, of December 13, on the protection of personal data (hereinafter, RLOPD) already contemplated as one of the basic level security measures that those responsible had to adopt in all treatments, that the *"security document must establish the periodicity, which in no case must be greater than one year, with which the passwords must be changed which, while they are valid, must be stored in an unintelligible way."*

It is worth noting that the security measures provided for in the RLOPD were enforceable until 05/25/2018, the date on which the RGPD came into force, which is why prior to that date the COPC had to have implemented the security measure consisting in establishing the periodicity of passwords provided for in article 93.4 of the RLOPD.

For its part, the RGPD regulates the principle of integrity (article 5.1.f RGPD) determining that personal data will be treated "in *such a way as to guarantee adequate security of personal data, including protection against non- authorized or illegal and against*

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

its accidental loss, destruction or damage, through the application of appropriate technical or organizational measures".

Also, 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 seriousness variables for the rights and liberties 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 accordance with the above, following the entry into force of the RGPD (25/05/2018), it is necessary to carry out an assessment of the risks involved in each treatment, in order to determine the security measures that must be implemented. According to the COPC, this assessment was carried out in September 2018 and, as a result of it, it was decided to start implementing the aforementioned security measure progressively until 02/19/2019.
However, until 04/30/2019, the implemented measure was not effective, as users with expired passwords were allowed to continue browsing the private space of the school website.

As indicated by the instructing person, during the processing of this procedure the fact described in the proven facts section, which is considered constitutive of the infringement provided for in article 83.4.a) of the RGPD, has been duly proven, which typifies the violation of *"the obligations of the person in charge and of the person in charge pursuant to 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 infringement in article 73.f) of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (hereinafter, 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:

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

"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".

As the instructing person explained in the resolution proposal, in the present case it becomes unnecessary to require the adoption of measures to correct the effects of the infringement, given that the COPC has left a record of the work that was carried out on 30 /04/2019 to ensure that users of the private space of the school website whose password had expired could not continue browsing.

resolution

For all this, I resolve:

1. Admonish the Official College of Psychology of Catalonia as responsible for an infringement provided for in article 83.4.a) in relation to article 32, both of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with what has been set out in the 4th legal basis.

2. Notify this resolution to the COPC.

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

4. 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 the provisions of 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.

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

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,