File identification

Resolution of sanctioning procedure no. PS 38/2022, referring to the Center for Telecommunications and Information Technologies

Background

1. On 11/25/2020, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Open Institute of Catalonia (hereafter, the IOC), which is the distance learning institute of the Department of Education, due to an alleged breach of the regulations on the protection of personal data .

In particular, the complainant stated that on 11/24/2020, when he was completing the electronic pre-registration procedure at the IOC, he refreshed the website and " *the personal data of another person I do not know appeared: your first and last name, your telephone number, your address, your date of birth, your DNI and your e-mail* ". The reporting person provided documentation about the events reported, specifically, an image of the computer screen at the time when the information related to *"Student data"* corresponding to a third person appeared.

2. The Authority opened a preliminary information phase (no. IP 361/2020), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to 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 were susceptible to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 12/18/2020 the reported entity was required to report on the reasons that on 11/24/2020, when the person reporting here processed the electronic pre-registration at the IOC, another user's personal data appears on the screen, and also about the security measures implemented by the institution to protect the confidentiality of the personal data of students who pre-register online, to prevent access by third parties to these personal data .

4. On 01/04/2021, the Department of Education responded to the above-mentioned request in a letter in which it set out, among others, the following:

- That *"On November 25, 2020, the Department's data protection representative receives a communication from the IOC management informing her that during the morning (of the same November 25) they had evidence of the existence of two incidents related to the data that dealt with future students in the virtual Secretariat* ."

- That " *Faced with this possible violation of security and as responsible for the treatment of the affected data, the director of the center had carried out the following actions:*
  a) He indicated to the students that the complaint was being handled , and that they would be informed of the
  resolution of the incident when it was resolved.
  b) Notified the incident and requested ***the Solutions Manager in the Department of CTTI Education that gave immediate instructions to block access to***

the Secretariat *where the incidents had been detected. They also notified the Sub-Directorate*
general of Administration and Organization of Public Centers.
c) Collected evidence and information regarding the extent of the incident (number of students, type of data accessed,...).
d) He ***required the Solution Manager at the Education Department of the CTTI because it is***
manage the resolution of the incident *as soon as possible and confirm to them that was solved and the Virtual Secretariat could be reopened again in good condition sure (...).*

- That the entity carried out a series of investigative actions on the facts reported, *"according to the Procedure proposed by the AEPD in the Guide for the management and notification of security breaches",* from the results of which it concluded that it was not necessary to notify the security breach to the monitoring authority.

- That " *On the afternoon of November 25 itself, the CTTI communicated that it had already found the incident in the application, that the database had also been reviewed to see how many cases could be affected and that they only had one (the reference one) and it had already been fixed. Also, a deployment package for the application was prepared so that the error was corrected and could not happen again with the expectation that everything would be uploaded the next day in the early hours. "*

- That " *On November 26, the Department's data protection representative received from the CTTI the detailed technical explanation of the problem that had already been resolved: on 11/24/2020, student AAA AAA AAA deregistered twice, once with a DNI X and her first and last name and another with a DNI Y and her first and last name . Since the DNI is the unique identifier for the file creation, both records were created. Linked to the registration, there is the process of creating the username (which must also be unique), and which is done with the combination of first and last name. In the first case, the correct username is created , but in the second, as it already exists, the system gives an error generating an empty username (" "). On the other hand, the student BBB BBB BBB registers for registration successfully and checks the status of your registration. In the meantime, he does other activities, so his time skips out of the page. The problem in this case is that instead of taking the student out of his session, as other pages of the Secretariat do (such as the itineraries), the username variable ceases to have value, that is to say it passes to be empty By having this empty username , when the user refreshes the page, an inconsistency is generated between the value of the variable and the empty record inserted in the previous double registration (from the AAA AAA AAA) and retrieves the data from another student (randomly), which has been those of the CCC CCC CCC _ Hence the student BBB BBB BBB could see the data of the student CCC CCC CCC .*"

- That " *To resolve the incident, the following were carried out actions :*
The empty value was removed from the database so that the situation could not be reproduced.
The source code of the application was modified so that, apart from controlling that usernames with a null value were not generated, they could also not be generated with the value " "). This modification was carried out on the same morning of November 26, leaving the problem definitively resolved ."

- The entity closes the allegations with the following conclusion :
  " *CONCLUSION:*
  The cause of the security breach did not come directly from the IOC but from its IT provider - the CTTI, which had a technical problem that caused the security breach. The solution also came from the IT provider who detected the technical cause and put the solution in place in a very short time .
  The IOC limited itself to immediately transferring the incidence to the IT provider, the CTTI and the Department of Education, the data protection delegate informed, in addition to taking the appropriate preventive measures (block the access to the virtual Secretariat) to prevent new ones from occurring while the solution was sought, and, finally, he apologized to the person reporting on his own behalf and to the Department."

5. On 03/22/2022, following the response of the IOC of the Department of Education in which it pointed to the Center for Telecommunications and Information Technologies (hereafter CTTI) as possibly responsible for the events, it was considered necessary request information from the CTTI, so that it reports, among others, on the following:

- if the security breach suffered, which would have allowed a person at the time of online pre-registration at the IOC to be able, through the web, to access data linked to third parties, would have occurred within the framework of a assignment entrusted to the CTTI, and in such case, provide the supporting documentation of this circumstance (contract of assignment signed with the IOC).
- the reasons that would explain that on 24/11/2020, when the person making the complaint was processing the electronic pre-registration at the IOC, the personal data of another user appeared on the screen.
- on the security measures implemented by the CTTI in the application developed to carry out online pre-registrations at the IOC, to prevent third parties from accessing this personal data.

6. On 04/26/2022, given that the deadline granted had been exceeded without the CTTI providing the required information, the request to the CTTI is reiterated and a new deadline of 5 days is granted to respond, with the express warning that failure to comply could result in an infringement of the regulations on the protection of personal data.

7. On 02/05/2022 , the CTTI complied with this requirement by means of a letter stating, among others, the following:

- That " *the security breach suffered would have occurred within the framework of the provision of ICT services that the CTTI provides to the Generalitat de Catalunya and its Public Sector. Specifically, within the framework of the assignment that the Department of Education entrusts to the CTTI, since the IOC depends on it, more specifically, it depends on the General Directorate of Public Centers. For this reason, we are attaching the personal data processing commission agreement in force between the CTTI and the Department of Education .*"

- That " root of a threat in the *application logout control , inherited in the application code of the previous CTTI application provider due to the obsolescence of versions in the code of the application, a lack of control was detected regarding the personal data sheet of the students. This caused that when a student lost the session, due to having passed more than ten minutes, the application did not redirect him to the expired session plan in which*

he had to log in again , instead, the student remained in the personal data sheet and the application code loaded the data of the next student from the search filter of these studies ."

- That " *on the security measures implemented, a new function was created in the application that controls the session time of each student who enters the personal data sheet, with a maximum time of 600 seconds (10 minutes), the which, if the indicated time runs out, redirects the students to the expired session plan of the IOC secretariat."*

- That " *as a result of this fact, an analysis was carried out in all the studies that could suffer from this lack of session control, in order to apply the same changes to the data files and other parts of the application where treat personal and sensitive data. Finally, it was only necessary to apply it in the data sheet of the reported studies.*

  Finally, indicate that both the Cybersecurity Agency and the CTTI act proactively through a risk mitigation plan regarding technological obsolescence."

The CTTI provided, together with its written response, a copy of the document " *Agreement for the processing of personal data between the Administration of the Generalitat, through the Department of Education and the Center for Telecommunications and Technologies of the Information from the Generalitat de Catalunya"* , formalized on 30/03/2016.

In said Agreement, it was established in the first clause that the object of the treatment order was the following:

" *Through this assignment agreement, the CTTI is authorized, in the capacity of data controller (hereinafter, data controller), to process, on behalf of the data controller (hereinafter, data controller) the necessary personal data for the centralized, transversal and coordinated management of ICT solutions in accordance with the Government Agreement of October 18, 2011* ".

Likewise, in the third clause, relating to the obligations of the person in charge of the treatment, the following was established, among other obligations:

"i) Comply with the security measures that correspond to the level of security that the person in charge has declared in Annex I of this order, according to what is established by the LOPD and the RLOPD and, in accordance with the following specifications:
(...)
i.7) Apart from these specifications, the person in charge must implement the set of measures provided for the high level of security in Title VIII of the Regulation of the Organic Law on the Protection of Personal Data, approved by the King decree 1720/2007, of December 21. "

In Annex I of this Assignment Agreement, where the files and protection levels subject to the processing assignment are related, a high level of security is established for the files relating to the students for whom I am responsible for the file the Directorate of the IOC.

8 . On 07/06/2022, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against the Center for Telecommunications and Information Technologies for an alleged infringement provided for in article 83.4.a), in relation to article 32.1.b); 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 06/09/2022.

9. On 20/06/2022, the CTTI made allegations to the initiation agreement , and provided a copy of the "Service incident report", dated 15/06/2022.

10. On 09/23/2022, the person instructing this procedure formulated a resolution proposal, for which he proposed that the director of the Catalan Data Protection Authority admonish the Center for Telecommunications and Information Technologies as responsible for an infringement provided for in article 83.4.a) in relation to article 32.1, both of the RGPD.

This resolution proposal was notified on 09/23/2022 and a period of 10 days was granted to formulate allegations.

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

proven facts

The Department of Education (responsible for the treatment), by virtue of the Commissioning Agreement formalized on 30/03/2016, commissioned the CTTI (responsible for the treatment) to treat on behalf of the person responsible for the treatment, the necessary personal data for the centralized, transversal and coordinated management of ICT solutions.

In this Agreement, the Department of Education established that the CTTI had to implement the security measures provided for in Annex I of the agreement, for each of the files detailed there. In the case of the IOC students, it was foreseen that the CTTI had to implement the security measures for the high level, in accordance with Royal Decree 1720/2007, of December 21, which approves the Regulation of the Organic Law 15/1999, of December 13, on the protection of personal data (hereinafter, RLOPD and LOPD, respectively)

CTTI did not adopt adequate security measures to ensure that IOC students could not access personal data of other students. Specifically, on 24/11/2020, while the complainant was pre-registering online for a course offered by the IOC, the personal data relating to another student appeared on the screen.

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 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. 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.

In this regard, it must be said that allegations that were formulated in the initiation agreement are not allegations in themselves tending to question or distort the reality of the facts that motivated the initiation of the procedure, nor their legal qualification , but focused, mainly, on exposing the corrective measure implemented by the entity in order to ensure that events such as those proven here do not happen again.

In this sense, the entity, on the one hand, literally recognizes " *its responsibility regarding the facts imputed as the person in charge of the processing of the personal data of the IOC related in Annex 1 of the Agreement d "treatment order signed between the CTTI and the Department of Education on March 30, 2016",* and on the other hand, it provides the document " *Incidence report of the service* ", which includes the chronology of events, the actions taken completed and the corrective actions and improvements implemented in order to ensure that the security incident does not happen again, and that IOC students cannot access other students' personal data electronically. It also reports that, following the events reported, the entity carried out an analysis of the rest of the system's applications susceptible to the same security incident, and the final result was that in none of the cases was the vulnerability repeated of security that would have allowed the facts proven here to happen. Lastly, the CTTI reports that with the Cybersecurity Agency they are proactively acting through a plan to mitigate risks towards technological obsolescence, and also, on the approval during the first quarter of 2021 of the " *First Security Program of the Department of Education* ", which establishes the creation of a security committee to be able to carry out a much more accurate monitoring of the existing risks in cyber security .

In this regard, it should be noted that this Authority positively assesses the different measures implemented by the entity, but it should be noted that the adoption of these measures does not distort the reality of the imputed facts or the correction of its legal qualification.

3. In relation to the facts 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 determining that personal data will be *" treated in such a way that security is guaranteed data adequacy _ personal , including the protection against unauthorized or illegal treatment and against it loss , destruction or accidental damage , through the application of measures technical or organizational appropriate (integrity and confidentiality)".*

On the other hand, article 32.1 of the RGPD, regarding data security, 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 variable probability and severity for the rights and freedoms of physical persons, the 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, which if applicable includes, among others:*

a) pseudonymization and encryption of personal data;
b) the ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems and services;

c) the ability to quickly restore availability and access to personal data in the event of a physical or technical incident;
d) a process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the treatment .

In this case, in the Processing Commission Agreement dated 03/30/2016, the data controller established that the security measures applicable to the files relating to IOC students had to be high-level security measures in accordance with the RLOPD.

In this regard, it should be borne in mind that on the date of the events reported, the content of the Processing Agreement dated 03/30/2016 was fully in force, given that according to the fifth transitional provision of the LOPDGDD, the data processor contracts signed before 05/25/2018 under the provisions of article 12 of the LOPD, remained in force until the expiry date indicated and in case it has been agreed indefinitely, until 05/25/2022.

This is how things are, and given that the validity of the referenced Commission Agreement is linked to the still valid Government Agreement of 18/10/2011, and that it is not known that either party has urged the modification of the Assignment agreement to adapt it to the provisions of article 28 of the RGPD, it must be considered that said assignment agreement remained in force until 05/25/2022, without it being required to adapt its content in article 28 of the RGPD.

However, it should be noted that, regardless of the validity of the referenced Commission Agreement, from the entry into force of the RGPD (25/05/2018), the security measures did have to be applied derived from the RGPD. In other words, those security measures which, following a prior risk assessment (art. 32 of the RGPD), are considered appropriate to guarantee a level of security appropriate to the risk.

Therefore, the CTTI had to implement, in relation to the processing of the personal data of the IOC students, the high level security measures involved in its processing .

In this regard, it should be borne in mind that the first additional provision of the LOPDGDD establishes the following: " *The National Security Scheme must include the measures that must be implemented in case of processing of personal data to avoid - its loss, alteration or unauthorized access, with the adaptation of the risk determination criteria in the processing of data to that established in article 32 of Regulation (EU) 2016/679"* .

Well, with respect to the conduct described in the proven facts section, it is inferred that the accused entity violated the security measure provided for in article 16 of the National Security Scheme in force at that time (RD 3/ 2010, of January 8), precept that regulates the authorization and control of access in the following terms: " *Access to the information system must be controlled and limited to users, processes, devices and other systems of information, duly authorized, restricting access to the permitted functions* ."

In this regard, it should be noted that when the Assignment Agreement between the Department of EDU and the CTTI (2016) was formalized, compliance with the security measures relating to authorization and access control was already contained in Annex I of said Commission Agreement. This is so because in Annex I, it was already established that, in relation to the processing of personal data of IOC students , high-level security measures had to be implemented . In this regard, it should be noted that, at that time, compliance with

high-level security measures cumulatively entailed compliance with basic and medium-level security measures. Therefore, compliance with the security measures relating to access control and identification and authentication, provided for as basic level security measures in articles 91 and 93 of the RLOPD, respectively, was considered included.

During the processing of this procedure, the fact described in the proven facts section, which constitutes the violation provided for in article 83.4.a) of the RGPD, which typifies the violation as such, has been duly proven of *"the obligations of the person in charge and of the person in charge "* , among which is the collection in article 32.1.b of the RGPD transcribed above, referring to the security of the treatment that guarantees confidentiality, integrity, availability and permanent resilience of treatment systems and services.

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

"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 of Regulation (EU) 2016/679"

4. As the CTTI is a public law entity attached to the Department of Territory's Digital Policy Secretariat, the regime provided for in article 77 LOPDGDD applies to certain categories of persons responsible or in charge of the treatment, among these, public law entities linked or dependent on public administrations.

In this sense, 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".*

In the present case, it becomes unnecessary to require corrective measures for the effects of the infringement since the measures adopted by the CTTI are considered sufficient and

appropriate in order to ensure that in the future events similar to those proven here are repeated.

For all this, I resolve:

1. Admonish the Center for Telecommunications and Information Technologies as responsible for an infringement provided for in article 83.4.a) in relation to article 32.1, 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 legal basis 4rt.

2. Notify this resolution to the Center for Telecommunications and Information Technologies.

3. Communicate the resolution 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.

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,