File identification

Resolution of sanctioning procedure no. PS 43/2022, referring to Badalona Serveis Assistencials, SA

Background

1. On 04/01/2021, the Catalan Data Protection Authority received a letter from a person for which he filed a complaint against Badalona Serveis Assistencials, SA (hereinafter, BSA), on the grounds of a alleged breach of the regulations on personal data protection.

Specifically, the complainant complained about alleged improper access to his medical history, carried out from the Municipal Hospital of Badalona - managed by BSA - by nursing staff. The aforementioned accesses would have been made on the days and times indicated below: April 13, 2020, at 03:09 a.m.; April 16, 2020 at 10:42 p.m.; and, April 17, 2020 at 11:39 p.m.

The complainant accompanied his complaint with the letter he sent to BSA on 11/13/2021, communicating that improper access to his medical history had been carried out, and with the response letter from the reported entity dated 12/24/2021, confirming that the three accesses " *have been deemed improper or not directly linked to a healthcare or epidemiological task".*

2. The Authority opened a preliminary information phase (no. IP 3/2021), 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 were capable of motivating the initiation of a sanctioning procedure.

3. In this information phase, on 02/20/2021, the reported entity was required to respond to several questions relating to the reported facts, among others, the justification of the reported accesses.

4. On 02/26/2021, BSA responded to the above-mentioned request in a letter in which it set out the following:

- That the three accesses had been carried out by the same person with a nursing staff profile.

- That it has not been possible to establish that the controversial accesses *"are justified by the performance of an assistance or diagnostic act. Therefore, BSA catalogs them as improper or not justified in a care or diagnostic task of the professional who performed them. (...) It has also been found that this lack of justification, based on the interviews held by the entity's human resources department with the professional involved, which certified that the worker did not act due to the his professional work".*

"the labor disciplinary procedure applicable to the worker author of the unauthorized access is being investigated . *(...)"*

The letter from the reported entity also made it clear that, as a result of the reported events, a series of corrective measures were being taken to prevent this type of behavior from occurring again among its staff. In particular, it highlights the preparation of training actions, especially aimed at professionals with access to the clinical history, as well as informative, on the good uses of the clinical history and the labor, administrative and criminal consequences associated with its misuse information

Finally, the entity also reported on the security measures implemented in order to guarantee the rights of the users of its services. By way of example, the entity claimed to have a record of access to clinical history, periodic audit systems tending to review these accesses, among others.

5. On 28/06/2022, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against BSA for an alleged infringement provided for in article 83.5.a) in relation to article 5.1 f); 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 07/11/2022.

6. In the initiation agreement, the accused entity was granted a period of 10 working days to formulate allegations and propose the practice of evidence that it considered appropriate to defend its interests.

7. On 07/25/2022, BSA made objections to the initiation agreement, providing various documentation with its writing.

8. On 10/11/2022, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority impose on BSA the penalty consisting of a fine of 2,000.- euros (two thousand euros), as responsible for the infringement provided for in article 83.5 a) in relation to article 5.1 f), all of them of the RGPD.

This resolution proposal was notified on 11/11/2022 and a period of 10 days was granted to formulate allegations.

9. On 11/21/2022, the accused entity submitted a letter to the Authority in which it acknowledges its responsibility for the alleged facts and attaches proof of the voluntary payment in advance of the monetary penalty that the investigating person proposed . Specifically, the accused entity paid, on 11/21/2022, 1,200.00 euros (one thousand two hundred euros), corresponding to the pecuniary penalty, once the reductions provided for in article 85 of the Law have been applied 39/2015.

proven facts

On the 13th, 16th and 17th of April 2020, with the details indicated in the previous 1st, a person with a nursing profile who provided services at the Municipal Hospital of Badalona - managed by Badalona Serveis Assistencials, SA - went access the medical history of the person reporting here, without their consent, and without these accesses being related to any healthcare or diagnostic action.

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.

The reported data processing falls within the competence of the Authority by virtue of article 3.f) of Law 32/2010, to the extent that the Badalona Municipal Hospital, managed by BSA, is part of the comprehensive system of public use of Catalonia - SISCAT - (Decree 196/2010, of 14 December, of the comprehensive health system of public use of Catalonia), and in this sense, provides public health services in concert with the Catalan Service of health.

2. In accordance with article 85.3 of the LPAC, both the recognition of responsibility and the voluntary advanced payment of the proposed monetary penalty lead to the application of reductions. The effectiveness of these reductions is conditioned on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction. For both cases, sections 1 and 2 of article 85 of the LPAC provide for the termination of the procedure.

Although it submitted objections to the initiation agreement, the accused entity has not made objections to the resolution proposal, since it has accepted to both options to reduce the penalty amount. However, it is considered appropriate to reiterate below the most relevant of the reasoned response that the instructing person gave to the allegations before the initiation agreement.

2.1 About the subject responsible for the infringement

The accused entity questioned that responsibility was attributed to it for the commission of an infringement for facts that materially would have been carried out by one of its employees - who, in the framework of the internal investigation, would have acknowledged having improperly accessed the medical history of the person making the complaint - and invoked in this regard sentence no. 188/2022 of the Third Chamber of the Supreme Court which, in literal terms, provides:

> " *The obligation to adopt the necessary measures to guarantee the security of personal data cannot be considered an obligation of result, which implies that if personal data is leaked to a third party there is responsibility regardless of the measures adopted and of the activity carried out by the person responsible for the file or the treatment".*

In relation to the above, BSA added that, unlike the obligations of results, in the obligations of means, " *the commitment that is acquired is that of adopting the technical and organizational means, as well as deploying a diligent activity in its implementation and use that allows to achieve the expected result with means that can reasonably be qualified as suitable and sufficient for its achievement, which is why they are called "obligations of diligence or behavior", which have have been carried out by the person responsible for the treatment in this case".*

Attached to the statement of allegations, the accused entity provided a statement signed by the Human Resources Director, dated 03/05/2021, through which the worker who carried out the reported improper access was informed of the imposition of a penalty of two days suspension of salary and work, for the commission of a less serious offence.

Well, as recalled by the Third Chamber of the Supreme Court, in judgment 188/2022, legal entities are responsible for the actions of their workers in such a way that objective responsibility is not established, but it is transferred to the legal entity the lack of diligence of its employees (for all, STC 246/1991, of 19 December fj2).

In relation to the above, it follows from BSA's allegations that the commission of the offense would be materially attributable to a worker who provides services to her organization However, in accordance with the RGPD and, especially, with article 70 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter, LOPDGDD), the responsibility for infringements in the field of data protection fall on those responsible or in charge of the treatments, and not on their employees. In literal terms, STS 188/2022 provides:

> *"Finally, it is appropriate to remember that legal entities are responsible for the actions of their employees or workers. An objective responsibility is therefore not established , but if the lack of diligence of its employees is transferable to the legal entity, in this sense STC 246/1991, of December 19 fj 2.*
> *This Supreme Court in its STS nº 196/2020, of February 15, 2021 (rec. 1916/2020) has had the opportunity to address the responsibility of an Administration for breach of the duty of security of personal data by acts of employees. In it, the opinion of the Trial Chamber was shared when it affirmed that "[...] the responsibility of the Administration holding and in charge of the file [City Council of San Sebastián] cannot be excused in its diligent action, separately from the action of its employees or positions, but it is the "culpable" action of these, as a result of the violation of the aforementioned obligations to protect the reserved character of personal data that grounds the responsibility of the former in the sanctioning scope of whose application it is; by acts "own" by their employees or positions, not by third parties[...]". Adding further that "The above does not mean, of course, that we are projecting on the recurring City Council a principle of objective responsibility, nor that the principle of presumption of innocence is violated, nor that we give a lucky chance of inversion of the burden of prueba. It simply happens that, being admitted in our Administrative Law, the direct responsibility of legal entities, which are recognized, therefore, as infringing capacity, the subjective element of the infringement is embodied in these cases in a different way to how it happens regarding of natural persons so that, as*

indicated by the constitutional doctrine that we have previously reviewed - SsTC STC 246/1991, of December 19 (FJ 2) and 129/2003, of June 30 (FJ 8) - direct blameworthiness derives of the legal property protected by the rule that is infringed and the need for said protection to be really effective and by the risk that, consequently, must be assumed by the legal entity that e is subject to compliance with said rule".

In accordance with the above, it is clear that the fact that a nursing professional acted negligently, accessing the medical history of the now complainant on three occasions, does not exempt BSA from its responsibility as the person responsible for the treatment of the data of patients and users of the Municipal Hospital of Badalona.

2.2 On the diligence of the data controller

The accused entity demonstrated that it had acted diligently in relation to the processing of personal data, and had periodically carried out audits to assess the degree of compliance with data protection regulations.

Regarding the imputed facts, BSA explained that it convened the relevant meetings and directed internal investigations in order to clear responsibilities and sanction the employee who improperly accessed the medical history of the now complainant.

In relation to the above, BSA added that staff who join the company are always informed of their obligations in terms of privacy, confidentiality and data protection. And, in relation to the previous one, he maintained that, following the incident, specific trainings have been carried out and conferences have been held to raise awareness of the importance of data protection in the healthcare field.

Well, this Authority evaluates very positively the actions carried out by the imputed entity, for the purposes of ensuring compliance with data protection legislation. However, without prejudice to what is established in the fourth legal basis of this resolution, these circumstances cannot exempt BSA from its responsibility for the violation of the data protection regulations that are sanctioned here.

2.3 On the applicable penalty regime

Next, the accused entity argued that, despite having the legal form of a limited company, it is a public organization made up of entirely public capital, which is included in the budget of the Badalona City Council and which is presided over by the Mayor himself from Badalona. Likewise, the accused entity argued:

"Because of the particularities about its composition that we have highlighted, BSA should fit within the regime applicable to the entities included in article 77.1. Specifically, those in section d), BSA being an organization clearly dependent on a public administration such as Badalona City Council. The imposition of a financial penalty on BSA would imply a financial penalty on the administrators themselves, which would imply a double harm: that originating from the infringement itself and that resulting from facing the financial penalty.

It seems to be the will of the legislator to protect the citizen from this double sanction that establishes a specific sanctioning regime for the public sector"

Regarding this allegation, first of all, it must be clarified that article 70 of the LOPDGDD determines which are the entities that remain subject to the sanctioning regime established in the RGPD and the LOPDGDD, a regime which, for what is of interest here, will apply to BSA as the person responsible for the processing of the personal data that has led to the initiation of this procedure.
Having said that, BSA defends that the special regime of article 77.1 d) of the LOPDGDD applies to it, which foresees not imposing financial sanctions on certain persons responsible or those in charge of the treatment who have violated the regulations and, in particular, on " *public bodies and entities under public law linked or dependent on public administrations".*

In this regard, it should be noted that the relationship of entities provided for in article 77.1 LOPDGDD is essentially based on the legal form/nature adopted by the active subject of the infringement, in such a way that, if the legislator had wanted the entities dependent or linked to a public administration, whatever their legal form, were subject to the regime provided for in article 77.1 of the LOPDGDD, I would have expressly included them in this closed list.

For the above, given that joint stock companies, whatever the origin of their share capital or the composition of their board of directors, are not included in the list provided for in article 77.1 of the LOPDGDD, it must be concluded that the the general penalty regime provided for in article 83 RGPD is applicable.

3. In relation to the facts described in the proven facts section, relating to improper access by a nursing professional, refer to article 5.1. f) of the RGPD, which regulates the principle of integrity and confidentiality, determining that the data will be " *treated in such a way as to guarantee an adequate security of personal data, including protection against unauthorized or illegal treatment and against accidental loss, destruction or damage, through the application of appropriate technical or organizational measures .*

On the other hand, article 5 of the LOPDGDD, in relation to the duty of confidentiality, establishes:

"1. Those responsible and in charge of data processing as well as all the people who intervene in any phase thereof are subject to the duty of confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.
2. The general obligation indicated in the previous section is complementary to the duties of professional secrecy in accordance with its applicable regulations (...)".

During the processing of this procedure, the fact described in the section on proven facts has been duly proven, which is constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies the violation of " *the principles básicos para el tratamiento ",* among which the principle of confidentiality is at the top.

The conduct addressed here has been included as a very serious infraction in article 72.i) of the LOPDGDD, in the following form:

"The violation of the principle of confidentiality established by Article 5 of this Organic Law"

4. In the absence of a BSA in any of the subjects provided for in article 77.1 of the LOPDGDD , the general sanctioning regime provided for in article 83 of the GDPR applies.

Article 83.5 of the RGPD provides for the infractions provided for there, to be sanctioned with an administrative fine of 20,000,000 euros at most, or in the case of a company, an amount equivalent to 4% as a maximum of the global total annual business volume of the previous financial year, opting for the higher amount.

Having said that, it is necessary to determine the amount of the administrative fine to be imposed.

According to what is established in article 83.2 of the RGPD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the instructing person in the proposed resolution, the penalty of two thousand euros (2,000 thousand euros). This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

As mitigating criteria, the concurrence of the following causes is observed:

- The limited number of accesses over time and that affect a single person (art. 83.2 to RGPD and 76.2 to LOPDGDD)
- The degree of responsibility of the person in charge or of the person in charge of the treatment, taking into account the technical or organizational measures that have been applied under the provisions of articles 25 and 32 of the RGPD (art. 83.2.c RGPD).
- The lack of benefits obtained as a result of the commission of the offense (art. 83.2.k RGPD and art. 76.2.c LOPDGDD).
- The immediate start of an investigation by the entity for the purpose of clearing possible responsibilities among its staff (art. 83.2.k RGPD).

On the contrary, as aggravating criteria, the following elements must be taken into account:

- Nature of the infringement (art. 83.2 GDPR). To the extent that the breach of the duty of confidentiality is imputed, classified as a very serious breach of data protection regulations.
- The category of personal data affected by the infringement (art. 83.2 g RGPD).
- The connection of BSA activity with the processing of personal data (art. 83.2.k RGPD and 76.2 b LOPDGDD). Given that the accused entity manages a municipal hospital, it must be stated that there is a close link between its activity and the processing of a considerable amount of personal data - not only of patients or users, but also of health personnel, and others professionals who can provide their services to the entity.

5. On the other hand, in accordance with article 85.3 of the LPAC and as stated in the initiation agreement, if before the resolution of the sanctioning procedure the accused entity acknowledges its responsibility or does the voluntary payment of the pecuniary penalty, a 20% reduction must be applied on the amount of the provisionally quantified penalty. If the two aforementioned cases occur, the reduction is applied cumulatively (40%).

As has been advanced, the effectiveness of the aforementioned reductions is conditional on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction (art. 85.3 of the LPAC, in *fine)* .

Well, as indicated in the antecedents, by means of a letter of 21/11/2022, the imputed entity has acknowledged its responsibility. And, on the same date, he paid in advance 1,200 euros (one thousand two hundred euros), corresponding to the amount of the resulting penalty, once the cumulative reduction of 40% has been applied.

6. Faced with the finding of the infringement provided for in art. 83 of the RGPD in relation to files or treatment of private ownership, article 21.3 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, empowers the director of the Authority for the resolution declaring the infringement to establish the appropriate measures so that it ceases or its effects are corrected.

In the present case, however, it becomes unnecessary to require corrective measures for the effects of the infringement given that the conduct refers to an isolated and specific event, with which the effects of the infringement would have been consummated.

For all this, I resolve:

1. To impose on Badalona Serveis Assistencials, SA the sanction consisting of a fine of 2,000.- euros (two thousand euros), as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1 f), both of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with the 6th legal basis.

2. Declare that Badalona Care Services has made the advanced payment of 1,200 euros (one thousand two hundred euros), which corresponds to the total amount of the penalty imposed, once the percentage of deduction of 40% corresponding to the reductions provided for in article 85 of the LPAC.

3. Notify this resolution to Badalona Serveis Assistencials SA .

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,