Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 49/2021, referring to Empresa Metropolitana de Gestión del Cicle Integral de l'Aigua, SA (Aigües de Barcelona).

Background

1. On 03/26/2021, the Catalan Data Protection Authority received a letter from Ms. (...) for which he filed a complaint against Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, SA (hereinafter, Aigües de Barcelona), on the grounds of an alleged breach of the regulations on the protection of personal data.

The complainant stated that since 2019 he started receiving bank receipts from Aigües de Barcelona to his bank account that were addressed to the names of other people. He provided the receipts that corroborated the facts reported.

2. The Authority opened a preliminary information phase (no. IP 124/2021), 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 05/20/2021 the reported entity was required to:

- Identify the person holding the water supply contract no. (...)
- Identified if he had evidence of the facts reported and, if so, explained how he had became aware of and the measures taken in relation to these facts.
- Indicate the reasons why he would have issued the receipts corresponding to the person making the complaint in the name of other people that would subsequently have been sent to the bank account number of the person making the complaint.
- Explain the system used for issuing receipts and subsequent sending to bank collection.

4. On 02/06/2021, Aigües de Barcelona submitted a letter in which it requested an extension of the deadline to provide the required information.

It was agreed to extend the period of 10 days granted to the reported entity to provide the required information for another 5 days.

5. On 18/06/2021, Aigües de Barcelona responded to the aforementioned request through a written statement in which it stated that:

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

- The holder of the aforementioned water supply contract was Mr. (...). On 23/01/2019, in relation to this contract, a change of direct debit was requested, with the owner of the associated bank account being the complainant.
- On 1/02/2021, the complainant called the customer service and warned that he was receiving receipts in which other people were identified. He was informed by Aigües de Barcelona that it was necessary for him to provide the bank receipts in order to be able to analyze the incidence more quickly, without prejudice to the fact that his request will be recorded and it was confirmed that he was only paying for the consumption that corresponded to him and that, in no case, he was paying invoices for other supply policies.
- On 9/02/2021, the complainant made the same claim through the Aigües de Barcelona website. But since the attached documents could not be opened, they requested them again in a different format. On 02/16/2021, the person sent the invoice, but not the bank receipts.

- On 05/05/2021 the telephone service operators raised the facts to a customer service manager of the company who immediately contacted the data protection officer.

- On 05/28/2021, the data protection representative issued a communication to the person reporting in which he informed that they had proceeded with the rectification.
- The cause of the incident had been a non-systematic and human error by some operators of the Customer Service Area who, when answering the call of service users, at the time of identifying them and verifying their data, in the case of new users and not being registered in the system, did not correctly apply the established procedure, that is to say, in the case of unregistered customers or users, a new customer/user had to be "created" and , instead of doing it this way, they "edited" the DNI of the reporting person (which was the last customer "file" edited and, therefore, the one that emerged by default). This led to the fact that in the bank remittance, associated with the claimant's account number, it was erroneously associated with the names and surnames of these new users. This happened in 11 invoices, which charge was debited to the account owned by the person making the complaint.

- The measures that have been adopted in relation to the events that have taken place, among others, are: the reporting person's customer record is deleted from the computer program and re-created with the correct data.
- Improvements have been made to the customer service procedure: on all customer/user screens, no customer/user is selected by default, but the customer service operator is forced to customer to search or create a new customer/specific user. It is thus guaranteed that it is not possible to "edit" when it does not correspond, which is what happened in the present case and the only possible options are "new" or "search", having deleted the option to edit".

The reported entity attached various documentation to the letter in support of its statements.

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

6. On 28/09/2021, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, SA (Aigües de Barcelona) for an alleged infringement provided for in article 83.5.a), in relation to article 5.1.e); 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 09/28/2021. On 09/10/2021 this notification was rejected by the system without the reported entity having accessed it.

On 25/10/2021 the notification was practiced again. The accused entity accessed it on 02/11/2021.

7. On 16/11/2021, Aigües de Barcelona made objections to the initiation agreement, which are addressed in section 2 of the legal foundations.

The accused entity provided various documentation with its letter.

8. On 01/13/2022, the person instructing this procedure formulated a proposed resolution, by which it was proposed that the director of the Catalan Data Protection Authority impose a penalty on Aigües de Barcelona consisting of a fine of 4,000 euros (four thousand euros), as responsible, for an infringement provided for in article 83.5.a) in relation to article 5.1.d), both of the RGPD.

This resolution proposal was notified on 20/01/2022 and a period of 10 days was granted to formulate allegations.

9. On 01/31/2022, the accused entity paid in advance 2,400 euros (two thousand and four hundred euros), corresponding to the monetary penalty proposed by the investigating person in the resolution proposal, once the planned reductions have been applied in article 85 of Law 39/2015.

10. On 02/04/2022, the accused entity submitted a letter in which it acknowledged its responsibility for the alleged acts and certified that it had made the voluntary advanced payment of the monetary penalty proposed by the investigating person.

proven facts

Between 21/09/2019 and 29/03/2021, Aigües de Barcelona issued a total of 12 invoices and the corresponding direct debit receipts with incorrect personal data.
Specifically, he assigned the names and surnames of 5 different users to the DNI of the reporting person. For this reason, the bank receipts were sent for collection to the bank account of the complainant with the names and surnames of different people to the bank account holder.

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

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.

Article 3 f) of Law 32/2010 is applicable, which provides that the scope of action of the Catalan Data Protection Authority includes the files and the treatments they carry out: f) The other entities of private law that provide public services through any form of direct or indirect management, if it concerns files and treatments linked to the provision of these services.

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 Aigües de Barcelona submitted allegations to the initiation agreement, it has not formulated allegations to the resolution proposal, since it has accepted both options to reduce the amount of the penalty. 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. Aigües de Barcelona admitted the events, but alleged that they had been caused by human error and alleged a lack of intentionality.

With regard to the cause of the issuance of receipts with erroneous data, the reported entity indicated as the cause a human error when applying the established procedures and stressed that it was not an error in the system . Regarding this, it should be emphasized that this human error would not have occurred if the system had the necessary controls to prevent the last used record from being edited by default. Indeed, the human error was possible because the customer management system (before applying the corrective measure that will be discussed later) displayed by default the last customer/ user record used and allowed data to be entered, as well how to rewrite existing ones.

Well, according to Aigües de Barcelona, this would have led some operators to enter in the customer file of the person reporting data of users who called by phone and who were not registered. It should be noted that in this case there were errors in 12 invoices and the corresponding bank receipts of the complainant.
In addition, these invoices and the corresponding bank receipts that should have gone to

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

name of the reporting person were issued with the first and last names of 5 different people. And even if there was no intention, it is considered that the imputed entity did not exercise the necessary diligence to prevent the error from occurring. Moreover, in this case it is not a one-off human error, but the error was repeated several times, in relation to data of several people, and also lasted for a long time (21/09/2019 and 29/03/2021).

It is considered that these errors would not have occurred if Aigües de Barcelona had adopted the appropriate control measures. Because a simple change in the customer management system would have prevented customer service operators from entering the data of other users in the reporting person's account. In fact, the accused entity already informed the Authority that it had adopted a corrective measure in the system to prevent events similar to the case at hand from occurring again. In particular, it was prevented from being able to edit the last used record and, after this change, when a user calls, he can only choose between two options: "New" or "Search". This prevents another user's data from being entered into another customer's record. Therefore, taking into account the above, it is considered that the imputed entity had not implemented in the customer management system the necessary controls to prevent customer service people from entering erroneous data into the system.

It should be remembered that the RGPD obliges the person in charge of the treatment to carry out an assessment of the risk of the treatment for the rights and freedoms of the natural persons affected by it and to adopt the technical and organizational security measures that are appropriate to guarantee an adequate level of security to the detected risk (article 32.1). In addition, it also obliges to carry out regular verification, evaluation and assessment processes to verify the effectiveness of technical and organizational measures in order to guarantee the security of the treatment (Article 32.1. d)). And with regard to the actions of the customer service operators who, according to the accused entity, did not follow the procedure established by the company at the same time as entering the data of the new users, it should be remembered that the same article 32.4 provides that the person responsible for the treatment must adopt measures to ensure that any person who acts under his authority and has access to personal data, can only process this data following instructions from the person responsible for the treatment. Well, in the case at hand it is clear that the accused entity had not implemented the necessary technical measures to avoid the risk of erroneous data being entered into the computer system, nor had it established the necessary controls to guarantee that the operators of customer service followed the procedures that the company claims to have implemented.

With regard to the lack of intentionality, it must be said that intent or intentionality is not an element of the type of infringing conduct. In fact, in matters of data protection, jurisprudence does not require that the infringing conduct has occurred with intent or intent, but rather that it is sufficient that negligence or a lack of diligence has intervened. It is necessary to cite, for all, the Judgment of the National Court of 02/05/2014 (RC 366/2012) issued in the matter of data protection, which holds that the condition of data controller

of personal data "imposes a special duty of diligence when carrying out the use or treatment of personal data or its transfer to third parties, as regards the fulfillment of the duties that the legislation on data protection establishes to guarantee the fundamental rights and public liberties of natural persons, and especially their honor and personal and family privacy, whose intensity is enhanced by the relevance of the legal assets protected by those rules."

It is for this reason that this plea is held to fail.

2.2. About the diligent performance of Aigües de Barcelona as data controller.

Subsequently, the accused entity alleged that its action had been diligent and proactive. That from the moment he became aware of the errors in the assignment of first and last names, the person responsible for customer service informed the Data Protection Delegate, so that he collaborated by providing the information and the background necessary so that the DPD could analyze the facts and issue a report.

However, this allegation cannot succeed, because from the time the complainant informed the Customer Service that he was receiving his bank receipts in the name of other people (02/01/2021) until the delegated person for data protection informed him that the erroneous data had been rectified (28/05/2021) almost four months passed. And from the time the complainant complained to the Customer Service until the responsible person contacted the delegated person for data protection (05/05/2021) three months passed. It should also be noted that the customer service asked the complainant to provide the incorrect receipts, which he provided, but when he could not open the file, he was insisted to provide them in other formats. The accused entity argued precisely that the reason why the complainant's complaint was not resolved earlier was that the person did not provide the receipts. However, this reason is not admissible because Aigües de Barcelona could perfectly consult its records to find out if the bank receipts (and invoices) it had issued and transferred to the account of the person here reporting were in his name or in the name of other people . Therefore, you should have adopted a proactive attitude in order to resolve the complaint in the shortest possible time. But it didn't until the data protection officer intervened. This is why it cannot be considered that Aigües de Barcelona had adopted a diligent and proactive attitude, given that for three months it did not take any action aimed at clarifying the facts and modifying the erroneous data. This violates the principle of data accuracy, because all reasonable steps were not taken to rectify erroneous data without delay. It should also be noted that the violation of the principle of data accuracy led to the disclosure of personal data of third parties (names and surnames) to the person making the complaint. In this sense, the violation of the principle of confidentiality of the data of the third parties affected is a consequence of the violation of the principle of accuracy of the data.

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

Among the documentation provided by the accused company, there was a report dated 05/06/2021 by the DPD person on the case in question. Those parts of the report that are of interest to the case being analyzed are transcribed below.

Description of the risks detected:

- Erroneous assignment of names and surnames to a customer file with the DNI of the person concerned, which has led to bank transfers to the account number of its owner with names and surnames that did not correspond. Therefore, the data was not accurate.
- User data has been disclosed, specifically, the first and last name to a third party, due to the association of their data with the DNI of the holder of the bank account (the reporting person), which has caused the Issuance of receipts with the first and last names that did not correspond, to which the person has had access.
- Delay in the detection of the violation of integrity and confidentiality.
- Delay in the attention of the right of rectification exercised by the interested person, in relation to the identification data that appeared on his bank receipt.
- Non-correct application of the requirements management procedures by some of the telephone service operators of Aigües de Barcelona.

Description of the proposed measures:

- Rectification and correct assignment of the name and surname of the interested person in relation to their bank details.
- Immediate attention to the right of rectification exercised by the person concerned, without the need to wait for the sending of the bank receipts.
- Remind the customer service operators of the obligation to apply the established and disseminated procedures.
- Incorporation of additional controls to those already in place, to track errors and help minimize the possibility of involuntary human errors by customer service operators.

- Application of improvements in the request handling procedure, removing the option to select a customer/user by default, in order to avoid errors in the execution of the procedure by some customer service operators.

In short, from the joint analysis of the facts considered proven and the documentation provided by Aigües de Barcelona, it is clear that the attitude of the data controller was neither proactive nor diligent. Accordingly, it is considered that his plea cannot succeed.

2.3 On corrective measures.

In its statement of allegations, the accused entity also informed the Authority of the specific corrective measures taken to prevent a similar security incident from occurring again.

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

Regarding the technical measures:

"- Elimination of the client/user of the SIEBEL program which associates clients and users (in this case, account holders not policy holders) with their bank account in order to avoid possible future errors.
- New creation in the client/user's SIEBEL program, incorporating the correct details of their name and surname, with respect to their ID and the bank account they own.
- Correct assignment of direct *debit* with the correct name and surname data of the SICAB (program used by *Aigües* de Barcelona to manage the billing process) so that the next bank receipts generated by the bank are correctly identified with the your first and last name associated with your account number".

Taking additional measures to track human error:

"- Auditing at the customer/user level (names and surnames) has been improved, in order to make it easier for the customer service operator and back office operators to analyze related incidents , improving the indicator register with the detail of any change made in the name-surname of the bank account.

- An improvement has been applied to the request handling procedure . On all customer/user screens, no customer/user is selected by default, but the customer service operator is forced to search for or create a specific new customer/user. It is not possible to "edit" when it does not apply. The option to edit has been removed."

Regarding organizational measures:

"On June 3, 2021, an information release was sent to operators to disseminate the improvements in the procedure.

The Customer Service proceeded to rectify the erroneous data and, on 05/28/2021, a communication was sent to the interested party that the request for rectification had been taken care of and an apology was sought for the delay".

The Authority positively assesses the technical and organizational corrective measures implemented in order to prevent a security incident similar to the one in question from occurring again. However, it must be clarified that the adoption of corrective measures does not distort the imputed facts. That is why, in accordance with what has been explained, it is estimated that this allegation cannot succeed.

3. In relation to the facts described in the proved facts section, relative to relative to the principle of rectification, it is necessary to go to article 5.1.d) of the RGPD, which provides that the data will be "d) accurate and, if necessary, updated; all reasonable measures will be taken

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

so that the personal data that are inaccurate with respect to the purposes for which they are treated are deleted or rectified without delay (''accuracy'')".

During the processing of this procedure, the fact described in the proven facts section, which constitutes the offense provided for in article 83.5.a) of the RGPD, which typifies the violation of "a) the basic principles for treatment, including the conditions for consent pursuant to articles 5, 6, 7 and 9".

The conduct addressed here has been included as a very serious infraction in article 72.1.a) of the LOPDGDD, in the following form:

> "a) The treatment of personal data in violation of the principles and guarantees established in article 5 of Regulation (EU) 2016/679."

On the other hand, as a result of the violation of the principle of accuracy, the principle of confidentiality has been violated, since data (names and surnames) of other people (a total of five) have been revealed to the person reporting

According to article 5.1.f) of the RGPD, personal data will be "treated in such a way as to guarantee adequate security of personal data, including protection against unauthorized or illegal processing and against its loss , destruction or accidental damage, through the application of appropriate technical or organizational measures". And article 83.5.a) of the RGPD, typifies as an infringement, the violation of: "basic principles of the treatment, including conditions for consent pursuant to articles 5, 6, 7 and 9". In turn, this behavior has been collected as a very serious infringement in article 72.1.i) of the LOPDGDD, in the following form: i) The violation of the duty of confidentiality established by article 5 of this Organic law."

In the present case, the violation of the principle of confidentiality necessarily follows from the violation of the principle of accuracy. Therefore, article 29.5 of the LRJSP is applicable, which provides that "When the commission of one infraction necessarily leads to the commission of another or others, only the penalty corresponding to the infraction must be imposed most serious crime." This is why conduct should only be sanctioned for violating the principle of accuracy.

4. As Aigües de Barcelona is a private law entity, the general penalty regime provided for in article 83 of the RGPD 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. This, without prejudice to the fact that, as an additional or substitute, the measures provided for in clauses a) ah) ij) of Article 58.2 RGPD may be applied.

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

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 4,000 euros (four 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 category of data affected (names and surnames) and the level of damages suffered by the affected persons (art. 83.2.a RGPD).
- The lack of intentionality (83.2.b RGPD).
- The lack of benefits as a result of the commission of the offense (art. 83.2.k RGPD and 76.2.c LOPDGDD).
- The technical and organizational measures adopted by the accused entity to avoid committing an offense like the one in the case at hand (art. 83.2.c RGPD).

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

- The nature and seriousness of the infringement, since the violation of the principle of accuracy has led to the disclosure of data of five affected persons (art. 83.2.a RGPD).
- Infractions previously committed by Aigües de Barcelona - sanctioning procedures numbers PS 26/2016, PS 36/2019 and PS 5/2020 (art. 83.2.e RGPD).
- Linking the offender's activity with the practice of processing personal data (art. 83.2.ki 76.2.b LOPDGDD).

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 dated 02/04/2022, the accused entity has acknowledged its responsibility. Likewise, on the same date he paid 2,400 euros (two thousand four hundred euros) in advance, corresponding to the amount of the penalty resulting once the cumulative reduction of 40% has been applied.

6. Given the findings of the violations provided for in art. 83 of the RGPD in relation to privately owned files or treatments, article 21.3 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, empowers the director of the Authority because the

resolution that declares the infringement establishes the appropriate measures so that its effects cease or are corrected.

In the present case, Aigües de Barcelona proved to have modified the erroneous data of the reporting person by deleting the client/user of the reporting person, creating a new one and incorporating the correct data. It also implemented an improvement in the customer management system that forced operators either to create a new user account when it came to unregistered users, or to search for the user, thus eliminating the possibility of selecting and edit the last customer record that appeared by default.

However, with regard to the records of the other affected users, whose names and surnames were attributed to the DNI of the reporting person, Aigües de Barcelona did not prove to the Authority that the records of these users had been configured correctly In the proposed resolution, it was proposed to require Aigües de Barcelona to certify the corrective measures implemented to ensure that the user records of these people had been configured correctly and that they did not contain erroneous or inaccurate data.

In this regard, in the letter dated 02/04/2022, Aigües de Barcelona explains that it has not been necessary take no additional corrective measures to those reported on the day, since the personal data of the other users were correctly registered in the system, that the error only affected the record of the reporting person. As he explains, when creating the record of a new user, the reporting person's file was edited (as if it were a template), but it was not taken into account that the name was changed in the reporting person's file and surnames. Once the corrective measures that were already reported to the Authority were taken, the problem was solved, but in no case have they ever found erroneous data in the records of the affected persons.

For all this, I resolve:

1. To impose on Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, SA the sanction consisting of a fine of 4,000 euros (four thousand euros), as responsible for an infringement provided for in article 83.5. a) in relation to article 5.1.d), 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 6th legal basis.

2. Declare that Aigües de Barcelona has made the advance payment of 2,400 euros (two thousand four hundred euros), which corresponds to the total amount of the penalty imposed, once

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

applied the 40% deduction percentage corresponding to the reductions provided for in article 85 of the LPAC.

3. Notify this resolution to Aigües de Barcelona, Empresa Metropolitana de Gestión del Cicle Integral de l'Aigua, 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 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.

The director,