

File identification

Resolution of sanctioning procedure no. PS 61/2022, referring to Ferrocarril Metropolità de Barcelona, SA of the TMB Group

Background

1. On 11/26/2021, the Authority received a letter in which a person made a claim against Ferrocarril Metropolità de Barcelona, SA (hereinafter, FMB) on the grounds of the alleged neglect of the right of access to your personal data. This rights protection procedure was assigned the number 147/2021, and ended with the resolution dated 04/01/2022, dismissing the claim, given that FMB certified that it had offered the claimant the possibility to access the personal data he had, thus responding to the specific terms of his request to exercise the right of access.

However, within the framework of the aforementioned procedure for the protection of rights, FMB, through a letter dated 02/01/2022, stated that it could not make available to the person making the claim the physical file relating to his person "because it could not *be located, since it was sent to an external archive, because it is a file with information between the years 1991 and 1994, and the company that managed it does not locate it*". The aforementioned letter was also accompanied by an email sent by the TMB Group to the claimant, on 12/11/2021, through which he was offered the possibility of accessing the " *little* " information contained in the TMB computer systems on your person.

2. The Authority opened a preliminary information phase (no. IP 122/2022), 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 1 October, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the fact that FMB had not been able to locate the physical file of the claimant, who had provided services to FMB, it was a consequence of a lack of appropriate technical and organizational measures and, therefore, likely to motivate the initiation of a disciplinary procedure.

In this preliminary information phase, the Authority incorporated the actions carried out in rights protection procedure no. 147/2021.

3. On 04/05/2022 and 04/07/2022 the Authority required the reported entity to report, among other issues, on the start and end date of the employment relationship between the person who requested access to their data and FMB, on the actions carried out in order to recover their personal data, and on the security measures required of the companies in charge of processing personal data, for the purposes of keep them and keep them safe.

4. On 04/22/2022, FMB responded to the above-mentioned request in writing in which it stated the following:

- That, " *after carrying out the tasks of investigation and consultation with the service provider, providing the file identification number, the provider answered that he did not find it in the indicated container. Wanting to corroborate this end, a person from FMB responsible for the physical archive was transferred, who confirmed that the file was not in the corresponding container. The supplier has indicated that with the security measures*

applied (see Annex II), the file could not be lost, at least it is likely that due to a one-off mistake in the numbering, it is filed in another container, and not in what should be there.

- That, the person concerned provided services to FMB SA, during the years 1991 to 1994.
- That, in FMB's computer systems, there is the information detailed below: "*name and surname of the worker, ID number, date of birth, place of birth, marital status, address, membership number, % working hours, working hours per day (theoretical), working hours per/week, working hours per month, working hours per year, working days per week, and professional categories*".
- That, "*due to the very seniority of the employment relationship with Mr. [...], once the usual legal deadlines in labor, tax or Social Security matters have expired, FMB only has a minimum of basic information according to the regulations on contracts for workers with asbestos, which is why the rest of the information goes to be opportunely suppressed at the time*".

The reported entity attached the data processor contract that FMB SA entered into with Iron Mountain España, SA, and in relation to which, argued that, "*this contract it was formalized on April 1, 2019 and covers all files that are the subject of an external file*".

5. On 07/10/2022, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against FMB SA for an alleged infringement provided for in article 83.4. a), in relation to article 32; all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free circulation thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 10/20/2022.

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 10/26/2022 the reported entity requested an extension of the deadline to present allegations to the agreement initiating the present sanctioning procedure, pursuant to article 32.1 of the 'LPAC.

8. On 27/10/2022 the Authority agreed to extend the deadline referred to in the seventh precedent, by five more days.

9. On 11/11/2022, FMB SA made objections to the initiation agreement, which are addressed in section 2 of the legal basis.

10. On 24/01/2023, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority impose on FMB SA the penalty consisting of a fine of 3,000.- euros (three thousand euros), as responsible for an infringement provided for in article 83.4.a) in relation to article 32; both of the RGPD.

This resolution proposal was notified on 01/25/2023 and a period of 10 days was granted to formulate allegations.

11. On 01/02/2023, the accused entity paid in advance 1,800.- euros (one thousand eight hundred euros), corresponding to the monetary penalty proposed by the investigating person in the resolution proposal, once the reductions provided for in article 85 of Law 39/2015.

12. On 06/02/2022, FMB SA submitted a letter to the Authority in which it acknowledges its responsibility for the alleged acts, and states that it has proceeded to make the voluntary advanced payment of the pecuniary penalty that the instructing person proposed

proven facts

FMB SA has not implemented appropriate organizational and security measures for the custody of its personnel data, which has prevented it from locating the physical file, relating to the employment relationship it maintained with the person who requested access to this information, request that gave rise to the rights protection procedure number 147/2021. On the one hand, in the framework of the claim procedure 147/2021, FMB stated that it could not locate the physical file with the information of the person making the claim. And, on the other hand, in the framework of the prior information phase that preceded this procedure, FMB has specified that the aforementioned documentation is not stored in the corresponding container.

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. 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 conditional 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.

The accused entity has not made any objections to the resolution proposal, as it has been accepted to both options to reduce the penalty amount. However, and given that he submitted allegations to the initiation agreement, it is considered appropriate to reiterate below the most relevant of the reasoned response that the instructing person gave to the allegations before the agreement d initiation.

2.1 On the existence of technical and security measures

The first section of the statement of allegations of the accused entity focused on defending that FMB SA applies " *appropriate technical and organizational and security measures for the custody of the data*".

In this regard, the accused entity pointed out that the data controller contract, concluded on 04/01/2019, with the company Iron Mountain España SA, specialized in the information custody service, complies with the requirements contained in article 28 of the RGPD. And, in relation to this, he added that said company has received the seal of compliance with the National Security Scheme, in accordance with Royal Decree 311/2022, which has the AENOR certifications for Information Security and Quality , and that has the appropriate technical and organizational measures to guarantee the confidentiality of the data it keeps. By way of example, FMB SA provided the company's policy " *oriented to the adoption of all*

those security measures that are considered logical to minimize potential risks in the processing of information", as well as a document detailing the procedure which governs access and referral flows of FMB employee records.

Among other considerations, the imputed entity claimed that it has a team dedicated to the maintenance of files - both of active employees and of those who have already caused termination - which classify the files of former employees, which are subsequently derive from the facilities of the person in charge of the treatment, and highlighted that, the health data is archived and kept outside the employee's work file.

Regarding the specific circumstances of the events that occurred, FMB SA stated the following:

"(...) Despite having implemented the detailed measures, in this particular case the physical file could not be located as a result of a specific human error: the file was located in a container of FMB that does not correspond to the noted reference (at this point it must be specified that it is FMB who takes care of placing the files inside the containers, and not the Treatment Manager, who does not access the contents) . Therefore, access to the file has not been made impossible due to a lack of implementation of measures or because these were incorrect, but rather the cause is a specific and specific error"

FMB invoked article 28 of Law 40/2015, of October 1, on the legal regime of the public sector, and cited judgment 188/2022 of the Third Chamber of the Supreme Court, judgment number 164/2005, of June 20, of the Constitutional Court and the judgment of April 26, 2002 of the National Court.

Having established the above, it should be borne in mind that the RGPD sets up a security system that is based on determining, following a prior risk assessment, which security measures are necessary in each case (Recital 83 and Article 32). So, for the purposes of analyzing and interpreting Article 32 RGPD, in relation to Recital 83 of the Regulation, its content is reproduced below.

Article 32 Security of treatment

" 1. 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 person in charge 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, where appropriate, 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".

2. When evaluating the adequacy of the level of security, particular consideration will be given to the risks presented by data processing, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to said data. (...)"

In turn, Recital 83 of the RGPD establishes that the security measures " *must guarantee an adequate level of security, including confidentiality, taking into account the state of the art and the cost of its application with respect to the risks and the nature of the data to be protected. When assessing the risk in relation to data security, the risks arising from the processing of personal data must be taken into account, such as the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or processed by another form, or unauthorized communication or access to said data, susceptible in particular to cause physical, material or immaterial damages and losses*".

Having established the above, in accordance with article 32.1 of the RGPD, FMB SA, as responsible for the treatment, must be able to guarantee the security and availability of the personal data for which it is responsible, prior implementation of appropriate measures to guarantee the level of security appropriate to the risks. And, the truth is that, in response to a request for access to its own data dated 10/29/2021, FMB informed the interested person that the physical file requested had not appeared " *in the external warehouse*" and offered him the possibility of " *coming to check the 'little' information contained in the computer systems*". Likewise, on 01/25/2022, within the framework of the rights protection procedure no. 147/2021, processed before this Authority, the accused entity acknowledged that it could not make available to the interested person the physical file relating to his person, due to the impossibility of locating it, a fact that led to the 'beginning of the preliminary information phase that preceded the present procedure.

Well, through the letter of allegations that FMB presented to the Authority on 11/11/2022, it stated that the reference file was filed in a container " *that does not correspond to the noted reference* ", as a result of human error. And, in this regard, he pointed out that, in accordance with sentence no. 188/2022, of February 15, 2022, of the Supreme Court, the establishment of technical and organizational measures constitutes an obligation of means and not of results, given the impossibility of ensuring the total elimination of risks. Said sentence, in its 3rd legal basis, provides the following:

"The obligation to adopt the necessary measures to guarantee the security of personal data cannot be considered an obligation of result, which implies that in the event of a leak of personal data to a third party there is responsibility regardless of the measures adopted and the activity deployed by the person responsible for the file or the treatment". (...) In the media obligations, the commitment that is acquired is to adopt the technical and organizational means, as well as to deploy a diligent activity in their implementation and use that tends to achieve the expected result with means that can reasonably qualify as suitable and sufficient for its achievement, therefore they are called "diligence" or "behavioural" obligations.

In this regard, without prejudice to the fact that the obligation to implement the technical and organizational measures that guarantee the security of the data can be considered an obligation of means, this does not exempt the person in charge from carrying out " *a diligent activity in his implantation y utilization* ", that is to say, that the measures implemented are appropriate and are used with diligence to achieve the desired result, diligence which, in the case at hand, had to be maximum taking into account that the information in question, such as has highlighted the file, it was not digitized in its entirety, so that, if the physical file was lost, the person concerned could not be guaranteed the availability or access to their personal data .

Having established the above, as argued in the proposal formulated by the person instructing this procedure, the object of this file is not about the generalized absence of security

measures, but what is imputed is that the technical and organizational measures implemented were not adequate to guarantee the availability of the data subject to treatment, and it is a proven fact, as recorded in the antecedents, that the physical file with the data of the interested person he has lost, in the sense that his whereabouts are unknown; that could not be made available to the person concerned; and that the accused entity, apart from assumptions, cannot assure with certainty the reason for its loss, nor has it provided any element that proves that the transfer of the file in question to the external archive took place in a time point after April 2019, when the contract with Iron was signed Mountain España SA, the moment to which it refers to the security measures it claims to have implemented.

For what is of interest here, FMB explained that, following the facts that have given rise to the present procedure, that is to say, after being aware that the Authority had agreed to start a preliminary information phase to determine the origin of starting a procedure sanctioning body, has adopted additional security measures to ensure the security of the file archive. As an example, he provided the Technical Instruction for the transfer of TMB labor files to the external archive, dated 09/01/2022, which establishes a double security mechanism in the file archive. This system consists of keeping a folder with the employee's work data, and before proceeding to its location in the corresponding container, entering the information in a coded and sealed envelope in order to guarantee that it is not opened and located. In this regard, the accused entity explained that, in order to ensure that the envelopes are stored in the corresponding containers, it has also established an additional verification and control system through sampling.

Well, the additional security measures adopted by the accused entity in the wake of the controversial events, show at least the need for FMB SA to strengthen and adopt organizational, technical and appropriate measures, in order to guarantee the security and availability of the data personal data subject to its processing, and consequently demonstrate, in accordance with the proven facts, that the measures that FMB SA had implemented up to that time were insufficient for the purposes of guaranteeing the availability of the personal data for which it is responsible.

For all of the above, it must be concluded that FMB SA's allegations cannot be successful in exonerating it from responsibility.

2.2 On the permanent nature of the infringement

Subsequently, the imputed entity argued that it is not possible to affirm that the imputed facts constitute a permanent infraction, as understood by the Supreme Court, in its judgment of November 4, 2013, when it describes it as "*those illegal behaviors that they persist over time and are not exhausted with a single act determining the maintenance of the illegal situation at the will of the author*".

In this regard, the reported entity considered that the imputed facts do not fit with the transcribed definition, given that it is not a behavior that persists over time, but rather that the loss of the file in question is a specific and specific event, which occurred as a result of human error. Likewise, he also argued that the situation would not have been caused voluntarily by FMB SA

Well, as stated in the proposal formulated by the person instructing this procedure, the facts that are imputed constitute a permanent infringement, in the sense that the technical and

organizational measures implemented by FMB SA have turned out to be insufficient to locate and make the disputed physical file available to the interested person. And this is a fact that persists over time, taking into account that, at the start date of the present sanctioning procedure, the data controller has not been able to locate the reference file, nor to make it available to the person interested in the personal data subject of your access request.

In accordance with what has been explained, it is estimated that this allegation cannot succeed either.

2.3 Individualization and graduation of the sanction

Reference is then made to the circumstances invoked by FMB SA for the purposes of mitigating any possible penalty, which will be analyzed in the 4th legal basis.

- Lack of intentionality or negligence in the commission of the offence.
- Nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operation concerned, as well as the number of affected interested parties and the level of damages suffered.
- Measures taken to alleviate the prejudices of the person concerned. In particular, FMB highlighted having been transparent with the interested person, informing him of all the progress in the search for the file, attending to him face-to-face, and having given him access to the requested data and contents of the computer system .
- Degree of responsibility of the data controller, taking into account the technical and organizational measures applied.
- Degree of cooperation with the control authority.
- The category of personal data affected by the infringement. In this regard, FMB SA explained that the disputed file does not contain special category personal data.

2.4 Precedents of this Authority and of the Spanish Data Protection Agency

Finally, FMB SA brought together different resolutions adopted by this Authority and by the Spanish Data Protection Agency (hereinafter, AEPD), in other complaint procedures.

Well, in this regard, and aside from noting that this Authority is not subject to the interpretive criteria adopted by the AEPD, with respect to which there is no subordination relationship, it should be noted that it is also not bound by its own resolutions when the the circumstances of the facts are substantially different and deserve, therefore, a legal assessment and a resolution that responds to the circumstances of each case.

Having said that, it should be made clear that neither the facts nor the concurrent circumstances, which are the subject of analysis in the resolutions invoked by FMB, issued in procedures E/08501/2019 and E/02434/2020 of the AEPD, and in the previous information no. 198/2019 of this Authority, and which all of them have in common their termination due to the archiving of the actions, do not coincide with the facts and circumstances that are the subject of this procedure.

For what has been said, this allegation cannot succeed in order to justify the filing of the facts reported here.

3. In relation to the facts described in the proven facts section, relating to the lack of implementation of appropriate organizational and security measures for the custody of the personal file, in physical format, of a former employee, 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 must be "*treated in such a way as to guarantee an adequate security of personal data, including the protection against the unauthorized or illegal treatment and against accidental loss, destruction or damage, through the application of appropriate technical or organizational measures*".

The RGPD particularly affects the obligation of the data controller to avoid the loss of information (Article 32.1 RGPD) as well as to guarantee its availability, in line with Article 5.1 f) of the same RGPD, transcribed previously .

This imputed fact is constitutive of the violation provided for in article 83.4 a) of the RGPD, which typifies the violation of "*the obligations of the responsible person and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43*", among which there is the one provided for in article 32.

In relation to the above, and given the circumstances of the case analyzed, it must be concluded that the security and technical measures implemented by FMB were not sufficient for the purposes of preserving the physical file with the data of the person concerned. This fact has prevented the accused entity from providing the aforementioned information in the rights protection procedure no. 147/2021, and in the preliminary information phase that preceded this sanctioning procedure. This lack of adequate security measures to guarantee the availability of the documentation requested by the interested person constitutes, as has been seen, a permanent infringement in the terms defined by the Supreme Court in its judgment of 04/11/2013 .

In accordance with the above, the LOPDGDD is applicable to the alleged facts, in accordance with the provisions of article 26.1 of Law 40/2015, of October 1, on the legal regime of the public sector ("*The sanctioning provisions in force at the time of the occurrence of the facts that constitute an administrative infraction are applicable*") which is also consistent with article 30.2 of the same rule ("*In the case of continuous or permanent infractions , the [prescription] period begins to run from the end of the infringing conduct*").

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

" g) Non-compliance, as a result of the lack of due diligence, of the technical and organizational measures that have been implemented in accordance with what is required by article 32.1 of Regulation (EU) 2016/679."

4. As Ferrocarril Metropolità de Barcelona SA does not comply with 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 83.4 of the RGPD provides for the infractions provided for there, to be sanctioned with an administrative fine of 10,000,000 euros at most, or in the case of a company, an amount equivalent to 2% 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 3,000 euros (three 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 has been considered:

- The nature and seriousness of the infringement, taking into account that, during the processing of the procedure, it has not been shown that, apart from the worker requesting access, it affected other employees of the company (art. 83.2.a RGPD).
- The measures adopted by the entity imputed for the purposes of alleviating the damages suffered by the affected person (art. 83.2.c RGPD). In this sense, FMB SA facilitated the access of the interested person to the data contained in the computer system.
- The lack of benefits obtained as a result of the infringement (art. 83.2.k RGPD and art. 76.2.c LOPDGDD).
- The lack of recidivism in the commission of infringements in the field of personal data protection (art. 83.2.e RGPD).

In this regard, as argued in the proposed resolution, the concurrence of other mitigating factors invoked by the accused entity should be ruled out, since the measures that FMB SA has implemented are necessary actions to preserve the security of the data ; the incident was not automatically notified to the Authority; and the required duty of care had to be maximum, when dealing with information with personal data, which was not digitized.

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

- Linking the offender's activity with the practice of processing personal data (art. 83.2.b RGPD).
- The damages suffered by the affected person to the extent that he cannot have the requested personal information, relating to his work activity during the years 1991 to 1994 (art. 83.2.a RGPD).

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 02/06/2023, the accused entity has acknowledged its responsibility. Likewise, it is certified that FMB SA has paid 1,800 euros (one thousand eight 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 for the resolution declaring the infringement to establish the appropriate measures so that its effects cease or are corrected.

In the present case, however, it becomes unnecessary to require corrective measures for the effects of the infringement, given that FMB SA has proven, within the framework of the present procedure, to have adopted corrective measures for the infringement consisting of strengthening the security of its employees' records.

For all this, I resolve:

1. Impose on Ferrocarril Metropolità de Barcelona, SA the sanction consisting of a fine of 3,000.- euros (three thousand euros), 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 6th legal basis.

2. Declare that Ferrocarril Metropolità de Barcelona, SA has made the advance payment of 1,800 euros (one thousand eight hundred euros), which corresponds to the total amount of the penalty imposed, once the 40% deduction percentage has been applied corresponding to the reductions provided for in article 85 of the LPAC.

3. Notify this resolution to Ferrocarril Metropolità de Barcelona, 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,