apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 22/2019, referring to SMS 91, SL.

Background

1. On 17/01/2019, Barcelona City Council notified the Catalan Data Protection Authority of a security breach (NVS 1/2019). Specifically, the Barcelona City Council informed that, on 11/01/2019, to a person who the Consistory claimed was an employee of the company Recerca i Desarrollo Empresarial, SL (hereinafter, RD Post), a company to which the City Council had ordered the provision of postal services, *notifications had "disappeared from inside the cart while he went upstairs to deliver a notification. The cart had to be left in the lobby of the building. He was able to retrieve some receipt notices later in the middle of the street, but not the documents."* In turn, Barcelona City Council numbered 10 notifications corresponding to the Municipal Institute of Finance of Barcelona City Council (hereafter, IMH).

The Barcelona City Council also provided various documents, including the complaint of the theft of the aforementioned cart, which the delivery person made on 11/01/2019 before the Police of the Generalitat-Mossos d'Esquadra (hereafter, PG -ME). This person, postman of SMS 91, SL on behalf of RD Post, stated in his appearance before the PG–
ME, among others, the following:

- That *"today, 11-01-2019, at about 11:30 a.m., Mr. (...) he was delivering the mail by the neighborhood of Can Serra de Hospitalet de Llobregat."*
- That *"Mr. (...) he carries a cart with a logo with the number of the company inside which is the correspondence and the certificates he has to distribute."*
- That *"Mr. (...) has entered the block located in calle (...), no. 4 de Hospitalet de Llobregat and up until that moment I had verified that both the certificates and the mail were inside the car without incident."*

- That *"he went up to a floor of the block and left the cart inside the lobby of the property."*
- That *"when he got off the floor in which he had to make a delivery, he continued his work normally."*
- That *"soon afterwards, during the delivery to a nearby school when the complainant wanted to continue handing out the relevant certificates, he noticed that the certificates that were inside the car had disappeared."*

- That *"at about 1:45 p.m., in front of the block (...), on Av Can Serra de Hospitalet de Llobregat, Mr. (...) he saw scattered the different certificates that had been taken from him inside his car."*

- That *"what Mr. (...) are the accusations of the delivery of said certificates, but not the content of them as (...) nominative notifications of the city council of Barcelona (...).*

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

2. The Authority incorporated the facts that are the subject of this notification of a security breach (NVS 1/2019) into the preliminary information phase (No. IP 274/2018) opened following the notification of another breach of security (NVS 23/2018), on 21/09/2018, by the City Council, also linked to the provision of postal services entrusted to RD Post.

3. On 07/29/2019, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against SMS 91, SL for an alleged violation provided for in article 83.4.a), in relation to the Article 32.1; both of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, 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 08/13/2019.

4. On 30/08/2019, SMS made objections to the initiation agreement.

5. On 25/11/2019, the instructor agreed to open a test period for a period of 10 days, in order to carry out the test consisting of requesting from SMS 91, SL, certain related information with the employment relationship of the person whose cart disappeared with correspondence on 01/11/2019; as well as documentation regarding the contractual relationship with Barcelona City Council or RD Post.

On the same day 11/25/2019, the notification of said trial agreement was made available to SMS 91, SL, through electronic means. This notification was considered rejected because 10 calendar days had passed since the notification was made available without its content being accessed, in accordance with article 43.2 of the LPAC.

6. On 09/12/2019 the instructing person agreed to open another test period for a period of 10 days, in order to carry out the test consisting of requiring certain information and documentation from RD Post to the effects of determining the eventual relationship with SMS 91, SL within the framework of the contract signed with Barcelona City Council for the provision of postal services.

On 09/12/2019 itself, the notification of said trial agreement was made available to SMS 91, SL and RD Post, through electronic means. This notification was considered rejected, in both cases, because 10 calendar days have passed since the notification was made available without its content being accessed.

7. On 12/18/2019 SMS 91, SL was notified, on paper, of the test agreement dictated by the instructing person on 11/25/2019, mentioned in the 5th precedent, in order to give compliance with what was required there within 10 working days.

In the same office, SMS 91 SL was also required so that, within the same period of 10 working days, it communicated to the Authority the necessary data to practice notifications by electronic means.

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

8. On 03/01/2020, SMS 91 SL provided the necessary data to practice notifications by electronic means.

9. After the period of 10 working days to comply with the provisions of the trial agreement notified on 12/18/2019, SMS 91, SL did not meet the request made there.

10. On 01/13/2020, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority impose on SMS 91, SL the penalty consisting of a fine of 3,000.- 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 13/01/2020 and a period of 10 days was granted to formulate allegations.

11. On 01/27/2020, the accused entity submitted a statement of objections to the resolution proposal.

proven facts

Of all the actions taken in this procedure, the facts detailed below are considered accredited.

On 11/01/2019, an employee of the company SMS 91, SL accessed the building located at street (...) no. 4 of l'Hospitalet de Llobregat in order to practice various notifications.
While this person went up several floors to attempt the notification practice, he left the cart containing various correspondence in the lobby of the building.

When he returned to the lobby, the cart had disappeared, which contained 10 notifications from the IMH addressed to citizens, some of them relating to administrative violations.

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.

2. The accused entity has made allegations both in the initiation agreement and in the resolution proposal. The first ones were already analyzed in the proposed resolution, but even so it is considered appropriate to mention them here, given that they are partly reproduced in the second ones. The set of allegations made by the accused entity are then analysed.

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

2.1. About the measures

In the 1st section of its statement of objections to the resolution proposal, the imputed entity alleged that it has implemented an integrated quality and information security management system based on the UNE EN ISO 27001:2013 standard. He added that the following clause was included in his distribution manual: *"10. Never leave shipments on public roads out of your control. If you have to deliver a certificate and there is no elevator, you must leave the cart inside the property and always carry the certificates with you."* In turn, SMS 91, SL
it stated that it complied with the principle of proactive responsibility, and to that end, it described a series of actions it carried out in this regard, some of which it documented.

The first thing to note about the document provided by the entity charged to accredit the certification of the integrated quality and information security management system based on the UNE EN ISO 27001:2013 standard is that it is dated 01 /09/2019, therefore, subsequent to the imputed facts (11/01/2019). And the second, that as indicated in that document, *"The company SMS 91 SL (...) is in the process of certification",* so it must be concluded that this certification has not yet been obtained.

Having said that, article 5.1.f) of the RGPD establishes that 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 , accidental destruction or damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality")."*

In turn, article 32.1 RGPD provides that *"the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk (...)".*

What Article 32.1 RGPD requires is that the security measures, which must be determined taking into account the risks arising from the loss or unauthorized access to the data (among others), must 'apply effectively.

That being the case, it is not a sufficient measure that in the delivery manual, it has been foreseen that the delivery person must take the notifications with them when there is no lift in a building. This measure provided for in the manual must be implemented effectively.

Well, in the specific case described in the proven facts section, and which was the subject of a security breach notification by Barcelona City Council, the security of the data was not effectively guaranteed, and in in particular, its proper custody to avoid loss or theft or unauthorized access to the correspondence subject to distribution. And, at this point, it should be noted that this custody obligation was also imposed by law

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

43/2010, of December 30, on the universal postal service, users' rights and the postal market (art. 6.1).

Indeed, the security of the data was compromised when, on 11/01/2019, an employee of SMS 91, SL left the cart containing the correspondence in the lobby of a certain building while attempting the practice of notifications on upper floors.

On the other hand, with regard to the measures of proactive responsibility detailed by the accused entity in its statement of objections to the proposed resolution, they do not allow the imputed facts to be distorted nor their legal qualification.

Lastly, it should be pointed out that the data protection impact assessment provided with the statement of objections to the proposed resolution was carried out on 06/03/2019. In other words, after the imputed facts (11/01/2019).

The same happens with respect to the documents of information and commitment of confidentiality, signed by the employees of SMS 91 SL on 11/07/2019, among which, it is worth saying that it is not recorded that it was signed by the delivery person to whom it disappeared the cart containing correspondence on 01/11/2019. Finally, with regard to the data protection policy, the security policy and the security document, this documentation has not been provided (in its statement of objections to the proposed resolution, the (the accused entity attached a document called *"SMS 91 SECURITY MEASURES",* which when opened showed the record of processing activities).

2.2.- About the risk

Next, SMS 91 SL transcribes in its statement of objections to the resolution proposal, the report of the security breach originated on 11/01/2019, indicating the estimation of the risk, for the purposes of *"evaluating the criteria indicated in articles 83.2 of the RGPD and 76.2"* of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD).

In advance, the fact that this Authority has become aware of the facts that have motivated the initiation of the present sanctioning procedure following the notification of the security violation by Barcelona City Council, once RD Post (in its capacity as 'in charge) notified him of the same, as a result of the prior communication of these facts by SMS 91, SL, must be a determining criterion when establishing the applicable penalty.

Having established the above, it is worth saying that the notification to the Authority is an obligation imposed on the data controller by article 33 RGPD in the face of any security breach, unless it is unlikely that said breach constitutes a risk for the rights and freedoms of natural persons.

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

Therefore, it should be noted that it is the person in charge who is responsible for assessing whether the security violations may constitute a risk to the rights and freedoms of natural persons, from which the obligation to notify the control authority is derived.

In this sense, the obligation of the person in charge (and subcontractor) is to notify the events subject to a security breach to the data controller (art. 33.2 RGPD), regardless of whether in their judgment it does not entail a probable risk for to the rights and freedoms of the people affected.

Notwithstanding the foregoing, several factors must be taken into account when assessing risk. In this respect, Recitals 75 and 76 of the RGPD suggest that, in general, when assessing risk, the likelihood and severity of the risk to people's rights and freedoms must be taken into account. And specifically, recital 75 RGPD determines the risks to the rights and freedoms of natural persons *"may be due to the processing of data that could cause physical, material or immaterial damages and losses, in particular in cases where the treatment may give rise to problems of discrimination, usurpation of identity or fraud, financial losses, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of pseudonymization or any other significant economic or social damage; in cases where the interested parties are deprived of their rights and freedoms or are prevented from exercising control over their personal data; in cases where the personal data processed reveal ethnic or racial origin, political opinions, religion or philosophical beliefs, membership in trade unions and the processing of genetic data, data relating to health or data on sexual life, or convictions and criminal offenses or related security measures; in cases where personal aspects are evaluated, in particular the analysis or prediction of aspects related to performance at work, economic situation, health, preferences or personal interests, reliability or behavior, situation or movements, in order to create or use personal profiles; in cases in which personal data of vulnerable persons, in particular children, are treated; or in cases where the treatment involves a large amount of personal data and affects a large number of interested parties."*

For the purpose of assessing the risk, SMS 91, SL uses the model provided in Annex III of the Guide for the management and notification of security breaches of the Spanish Data Protection Agency (hereafter, AEPD).

At this point, it should be emphasized that the Catalan Data Protection Authority and the AEPD are related based on the principle of collaboration, without any kind of hierarchy or dependency between them, so that the decisions or criteria of the AEPD do not bind this Authority, without prejudice to the existing instruments for the purpose of coordinating criteria.

Without prejudice to the above, the model contemplated by the AEPD as a reference in making the decision to notify the violation to the Authority and, where appropriate, to communicate it to the persons

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

affected, is for guidance as set out in the guide itself. In turn, this orientation model starts from the analysis of three parameters: the volume, typology of the data and the impact.

Having said that, the Working Group of Article 29 (hereinafter, WG29) in its guidelines on the notification of security breaches of personal data according to the RGPD (WP 250), recommends taking into account the following criteria: the type of violation; the nature, degree of sensitivity and volume of personal data; the ease of identifying people; the severity of the consequences for those affected; the special characteristics of the data subject; the special characteristics of the data controller; and the number of people affected.

And, in application of these (and contrary to the assessment carried out by SMS 91 SL), it is considered that the notification of the security breach to the Authority was required, given that the risk to the rights and freedoms of the people affected was not improbable. Among others, it is necessary to take into account the ease of identifying the affected persons, the possibility that the violation could lead to impersonation situations or the damage to the reputation of the affected persons (in particular, of the persons charged in a disciplinary procedure).

In any case, it should be reiterated that the risk assessment corresponds to the person responsible for the treatment.

2.3. About guilt

Subsequently, the accused entity invokes in its statement of objections to the proposed resolution the lack of guilt, which it considered not to be proven; as well as lack of intentionality.

In this regard, this Authority has recalled in several resolutions (for all, the resolution of sanctioning procedure no. PS 52/2012 - available on the website apdcat.gencat.cat) the jurisprudential doctrine on the principle of culpability, both of the Supreme Court, like the Constitutional Court. According to this doctrine, the sanctioning power of the Administration, as a manifestation of the *"ius puniendi"* of the State, is governed by the principles of criminal law, and one of its principles is that of guilt, incompatible with a regime of objective responsibility without fault.

In this sense, the Supreme Court in several rulings, all of 16 and 22/04/1991, considers that from this element of culpability it follows that the action or omission classified as an administratively punishable offense must be in all case imputable to its author due to grief or imprudence, negligence or inexcusable ignorance. Also the National Court (AN), in the Judgment of 06/29/2001, precisely in matters of personal data protection, has declared that to appreciate this element of guilt: *"simple negligence or failure to fulfill duties is enough that the Law requires the persons responsible for files or data processing to exercise extreme diligence...".*

Also of interest is the Judgment of the National Assembly of 08/10/2003, which explains the following:

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

"Therefore, contrary to what is ordered in art. 11.1 of Law 15/1999, of December 13 on Protection of Personal Data, the appellant entity communicated personal data to a third party without the consent of the affected person, without meeting the causes established in section 2 of that article for that consent is not required, and without his conduct being covered by art. 12 of the same Law.

SIXTH

For what affects culpability, it must be said that generally this type of behavior does not have a malicious component, and most of them occur without malice or intentionality. It is enough to simply neglect or fail to comply with the duties that the Law imposes on the persons responsible for files or data processing to exercise extreme diligence to avoid, as in the case at hand, a processing of personal data without the consent of the person concerned , which denotes an obvious lack of compliance with those duties that clearly violate the principles and guarantees established in Organic Law 15/1999, of December 13, on the Protection of Personal Data, specifically that of the consent of the affected person."

Likewise, the judgment of the Supreme Court of 25/01/2006, also issued in the area of data protection, is based on the required diligence and establishes that intentionality is not a necessary requirement for a conduct to be considered guilty .

With regard to the degree of diligence required, the Judgment of the NA of 14/12/2006 declared: *"the Supreme Court considers that imprudence exists whenever a legal duty of care is disregarded, that is, when the infringing subject does not behave with the required diligence. And the degree of diligence required must be determined in each case in attention to the concurrent circumstances, such as the special value of the protected legal property, the professionalism required of the infringer, etc."*

In short, it is necessary that in the conduct that is imputed there must be an element of culpability, but in order for culpability to exist it is not necessary that the facts have occurred with intent or intent, but it is sufficient that negligence has intervened or lack of diligence, as would be the case analyzed here. And it is worth saying that the duty of care is maximum when activities are carried out that affect fundamental rights, such as the right to the protection of personal data. This has been declared by the Judgment of the NA of 05/02/2014 (appeal no. 366/2012) issued in matters of data protection, which maintains that the status of person in charge of processing personal data *"imposes a special duty of diligence when carrying out the use or treatment of personal data or its transfer to third parties, in what concerns the fulfillment of the duties that the legislation on data protection establishes to guarantee the fundamental rights and public liberties of the physical 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."*

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

In turn, it should be noted that the wording given to article 28 of Law 40/2015 to the principle of responsibility or culpability, in which the mention of *"simple non-compliance" was deleted,* did not substantially alter the situation previous, in which the majority jurisprudential doctrine already had to be taken into account, in which the presence of the element of grief or guilt was already required, so that the idea of sanctioning based on a kind of of "objective responsibility". We have a sample of this jurisprudential doctrine in the judgment of the Supreme Court of 04/28/2016, in which art was obviously applied. 130 of the LRJPAC:

> *"Regarding the absence of intent or guilt in the commission of the offense, and the concurrence of good faith, we must point out that guilt as a principle of the sanctioning power provided for in article 130 of Law 30/1992, entails that " only the physical and legal persons who are responsible for them, even for simple non-observance, may be sanctioned for acts constituting an administrative infraction. This requirement, in the exercise of the sanctioning power, supposes that the conduct to be deserving of a sanction must involve the will or fault of the subject to whom it is imputed, because we are not in a system of objective responsibility unrelated to culpability, as deduces from the indicated article 130, and according to which this Chamber is declaring with a reiteration that excuses the quote".*

Based on the jurisprudential doctrine presented, SMS 91, SL is guilty of the lack of due diligence in not guarding a cart with correspondence, leaving it in the lobby of a building while the practice of notifications on the upper floors was attempted.

3. In relation to the facts described in the proven facts section, relating to data security, it is necessary to refer to article 32.1 of the RGPD, which 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 individuals, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk (...)."*

In relation to the provision of postal services, SMS 91, SL, did not guarantee the correct custody of the 10 IMH notifications that were in the cart that was left in the lobby of the building previously identified on 11/01/ 2019, since it did not implement any measures to prevent its theft or unauthorized access.

As indicated by the instructing person, during the processing of this procedure the facts described in the proven facts section, which are constitutive of the infringement provided for in article 83.4.a) of the RGPD, have been duly proven, which typifies as such the violation of *"the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43",* among which there is that provided for in article 32 RGPD.

Having said that, the conduct addressed here has been included as a serious infringement in article 73.g) of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter, 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 SMS 91, SL is a private law entity, the general penalty regime provided for in article 83 of the RGPD applies. Article 83.4 of the RGPD provides for a maximum fine of 10,000,000 euros, or in the case of a company, an amount equivalent to a maximum of 2% of the total annual business volume total of the previous financial year, opting for the higher amount.

For its part, article 83.2 of the RGPD determines the following, regarding the graduation of the amount of the administrative fine:

> *"2. The administrative fines will be imposed, depending on the circumstances of each individual case, as an additional or substitute for the measures contemplated in article 58, section 2, letters a) ah) yj). When deciding the imposition of an administrative fine and its amount in each individual case, the following shall be duly taken into account:*
>
> *a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operation in question as well as the number of interested parties affected and the level of damages and losses they have suffered;*
>
> *b) intentionality or negligence in the infringement;*
> *c) any measure taken by the person responsible or in charge of the treatment to alleviate the damages and losses suffered by the interested parties;*
> *d) the degree of responsibility of the person in charge or of the person in charge of the treatment, given the technical or organizational measures that have been applied by virtue of articles 25 and 32;*
> *e) any previous infringement committed by the person in charge or the person in charge of the treatment;*
> *f) the degree of cooperation with the control authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
> *g) the categories of personal data affected by the infringement;*
> *h) the way in which the control authority became aware of the infringement, in particular if the person in charge or the manager notified the infringement and, if so, to what extent;*
>
> *i) when the measures indicated in article 58, paragraph 2, have been previously ordered against the person in charge or the person in charge in relation to the same matter, the fulfillment of said measures;*

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

j) adherence to codes of conduct under article 40 or certification mechanisms approved under article 42, and
k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as the financial benefits obtained or the losses avoided, directly or indirectly, through the infringement."

In turn, article 76.2 of the LOPDGDD provides that, apart from the criteria established in article 83.2 RGPD, the following can also be taken into account:

"a) The continuing nature of the infringement.
b) Linking the offender's activity with the practice of processing personal data.

c) The profits obtained as a result of the commission of the infringement.
d) The possibility that the conduct of the affected person could have led to the commission of the offence.
e) The existence of a merger process by absorption subsequent to the commission of the infringement, which cannot be imputed to the absorbing entity.
f) Affecting the rights of minors.
g) Have, when not mandatory, a data protection delegate.
h) The submission by the person in charge or person in charge, voluntarily, to alternative conflict resolution mechanisms, in cases where there are disputes between them and any interested party."

In the present case and taking into account that there is no evidence that the accused entity had implemented the appropriate technical and organizational measures in accordance with what is established in articles 25 and 32 of the RGPD (article 83.2.d RGPD) previously to the imputed facts (11/01/2019), beyond the distribution manual that the imputed entity does not certify to have brought to the attention of the employee from whom the cart was stolen, the penalty of an administrative fine cannot be replaced by the reprimand sanction provided for in article 58.2.b) RGPD.

Once the application of the reprimand as a substitute for the administrative fine has been ruled out, the amount of the administrative fine to be imposed must be determined. According to the provisions of article 83.2 of the RGPD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, a penalty of 1,500
euros (one thousand five hundred 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 reduced number (10) of affected people (art. 83.2.a RGPD).
- The lack of intentionality (art. 83.2.b RGPD).
- The category of personal data affected by the infringement - there is no evidence that it affected special categories of data - (art. 83.2.g RGPD).

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

- The lack of benefits as a result of the infringement (art. 83.2.k RGPD and 76.2.c LOPDGDD).
- The measures adopted by SMS 91, SL subsequent to the imputed facts, which have been detailed in the 2nd legal basis, to which should be added the document by which the employees were informed of the security incident that is the subject of this procedure and clause 10a of the distribution manual was transcribed (83.2.k).
- And, especially, that this Authority became aware of the facts imputed as a result of the notification of the security breach by the Barcelona City Council, following the notification made by RD Post as the person in charge of the treatment, as a result of the prior communication of these facts by SMS 91, SL (art. 83.2.h).

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

- Negligence in the infringement (art. 83.2.b RGPD).
- Linking the offender's activity with the practice of processing personal data (art. 76.2.b LOPDGDD).

5. 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, no measure should be required to cease or correct the effects of the infringement, given that SMS 91 SL does certify a series of measures implemented after the date of the imputed facts tending to prevent the situation imputation is reiterated.

resolution

For all this, I resolve:

1. To impose on SMS 91, SL the sanction consisting of a fine of 1,500.- euros (one thousand five hundred euros), as responsible for an infringement provided for in article 83.4.a) in relation to article 32 , both of the RGPD.

2. Notify this resolution to SMS 91, SL.

3. 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

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

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,