File identification

Resolution of sanctioning procedure no. PS 34/2022, referring to the Catalan Society for Mobility, SA.

Background

1 . On the dates 05/10/2021, 06/10/2021, 07/10/2021, and 26/10/2021, the Catalan Data Protection Authority received up to six complaints made separately by citizens against the Autoritat del Transport Metropolità (henceforth, the ATM), and a complaint filed against the Societat Catalana per la Mobilitat, SA, (henceforth, SocMobilitat), on the grounds of an alleged breach of the regulations on protection of personal data.

Specifically, the complainants complained that on 05/10/2021 a security vulnerability had been detected on the T-mobilitat.atm.cat portal (https://t-mobilitat.atm.cat) which would have allowed access by third parties to their personal data recorded there, provided to register as users of the new T-Mobilitat card. Likewise, they complained that the detected vulnerability allowed the modification of user information contained there. In order to justify the facts reported, the reporting persons provided various documentation.

2 . Likewise, the ATM, in compliance with the provisions of article 33 of 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 treatment of personal data and the free circulation thereof (hereafter, RGPD), and in its capacity as data controller, notified this Authority on 10/06/2021, of the data security breach suffered (NVS 86 /2021), consisting of the vulnerability detected in the T-mobilitat.atm.cat portal, which compromised personal data of users registered there. The actions carried out in the framework of the notification of the said security violation (NVS 86/2021), were incorporated into the open prior information phase due to the complaints presented to the Authority for the same facts.

3 . On 10/01/2022, the Director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against SocMobilitat - (...)-, in order to resolve its alleged responsibility for the violation of the security principle of the data in the deployment of the T-Mobilitat web portal, and consequent violation of its confidentiality that had been the subject of a complaint.

This procedure was initiated against SocMobilitat , given that the result of the investigative actions carried out in the framework of the previous information opened by this Authority, it appeared that the facts object of imputation required within the scope of its responsibility, by virtue of the contract for the processing of personal data signed between the ATM (responsible for the processing) and SocMobilitat (awardee of the contract and in charge of the processing) on 09/30/2021, for the provision of the service of implementation and management of the new tariff system integrated with contactless technology (T-mobility card).

4. From the documentation provided by SocMobilitat in the processing of the sanctioning procedure -(...)-, it was found that the facts reported, that is to say, the alleged violation of the principle of data security in the deployment of the T portal -Mobility and consequent violation of its confidentiality , due to the lack of implementation of basic level security measures, were imputable to Indra Sistemas SA within the framework of the personal data processing contract signed between SocMobilitat (in charge of the treatment) and Indra Sistemas SA

(shareholder of SocMobilitat and sub-responsible for the treatment), for the provision of services in the implementation and management phase of T-mobility (among them, the deployment of the web portal) , in accordance with the data protection responsibility regime established in article 28.10 of the RGPD, which is also applicable to the sub-processor in accordance with articles 28.4 of the RGPD and 70.1.b) LOPDGDD .

Thus, in the personal data processing commission contract signed between SocMobilitat and Indra on 09/30/2021, the security measures that Indra had to adopt for the service subject to the commission were stipulated:

"7. Obligations of the data controller (...)
"7.5. Safety of Treatment
The treatment manager will implement the measures appropriate regarding the security of the Treatment , which correspond to those of the contracting Administration and which conform to the National Security Scheme (***BASIC LEVEL*** *).*

In any case, the Manager must implement mechanisms to:
a. Guarantee confidentiality , integrity , availability and resilience _ permanent treatment systems and services . _ _
b. Quickly restore availability and access to Personal Data , in the event of an incident physical or technical .
c. Verify, evaluate and assess regularly, the effectiveness of the measures technical and organizational implanted to guarantee the safety of the treatment .
d. Pseudonymize and encrypt personal data , if applicable .

Together, you must adopt all of them those others Measures that, taking into account the set of treatments it carries out, are necessary to guarantee a level of security appropriate to the risk .

Documentation related to risk management , including the results of audits _ periodicals that are carried out , can only be requested in any momento por el Tratamiento .(...).”

As stated in the agreement to initiate the sanctioning procedure (...) regarding SocMobilitat , the security measures that were violated in the configuration of the access control to the T-mobility portal, which they enabled access to remain open, and in turn, accessible to third parties, are of a basic level (section 4.1.2 "Security Architecture", section 4.2 relating to access control, and section 4.3.2 relating to the "security configuration") of the National Security Scheme (ENS) approved by Royal Decree 3/2010, to which reference is made.

In view of all the above, and in accordance with article 20.1.c) of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat of Catalonia, dated 27/05/2022 the Director of the Catalan Data Protection Authority resolved, in accordance with the principle of congruence that governs the sanctioning procedure, to declare the dismissal of the procedure (...) initiated against SocMobilitat, given that this entity does not would be responsible for the lack of application of the basic level measures that Indra was required to adopt , as stipulated in the treatment order contract signed between both entities on 09/30/2021.

However, from the documentation in the file it was clear, as corroborated by the report dated 11/05/2022 of the Technology and Information Security Area of the Authority, that

SocMobilitat would not have categorized or determined adequate risk level of the information system (categorized as basic level in point 7.5 previously transcribed of the contract in charge of the treatment) for the provision of the services entrusted to Indra in the implementation and management phase of the card T-mobilitat, reason for which, in said resolution, it was also agreed to initiate a new sanctioning procedure against SocMobilitat , for the purpose of resolving its responsibility for alleged violation of article 32 of the RGPD in the determination of the measures appropriate to the risk involved in the processing of data entrusted to Indra , and incorporate in the file, the actions and documentation involved in the sanctioning procedure (...).

5. On 01/06/2022, by agreement of the director of the Catalan Data Protection Authority, the present sanctioning procedure was initiated against SocMobilitat , for an alleged infringement provided for in article 83.4.a), in relation to article 32.2; all of them from the RGPD. This initiation agreement was notified to the imputed entity on 06/06/2022.

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, a period that was extended by another 5 days upon request from SocMobilitat .

6. On 06/27/2022, SocMobilitat filed objections to the initiation agreement .

7 . On 09/09/2022, the instructor of this procedure formulated a resolution proposal, for which she proposed that the director of the Catalan Data Protection Authority impose a fine of 10,000 euros on SocMobilitat as responsible , 'an infringement provided for in article 83.4.a) in relation to article 32.2, regarding the principle of data security, both of the RGPD.

This resolution proposal was notified on 09/13/2022 and a period of 10 days was granted to formulate allegations.

8. On 09/27/2022, the accused entity submitted a statement of objections to the resolution proposal.

proven facts

On 30/09/2021 the Catalan Society for Mobility, SA, formalized a data controller contract with the company Indra Sistemas, SA, for the provision of services within the framework of the T-mobility Technology Project, in accordance with the tasks assigned in the service contracts for the implementation and management phase dated 07/24/2014, and their subsequent modifications (clause 2a of the commission contract "Conditions and purposes of treatment ”):

"2. Conditions and purposes of the treatment
2.1 "The treatment will consist of the benefits techniques within the Project technology of T-Mobility attributed and assumed by INDRA in the contracts for the provision of services for the implementation phase for T-Mobility and in the provision of services for the management phase for T-Mobility signed between SOC MOBILITAT and INDRA on July 21 , 2014 and above later modifications addenda ."

The execution of these services involved Indra accessing and managing the personal data of T-mobility users, which would include sensitive data, and even special categories of data, in accordance with what is stipulated in the clause 3 of the order contract (“ Identification of the information affected, objeto de tratamiento ”).

With regard to the security measures that Indra had to implement or adopt for the provision of the commissioned services, the following security measures were required in the data processor contract signed between SocMobilitat and Indra :

"7. Obligations of the data controller (...)
"7.5. Safety of Treatment
The treatment manager will implement the measures appropriate regarding the security of the Treatment , which correspond to those of the contracting Administration and which conform to the National Security Scheme (***BASIC LEVEL*** *) (...).”*

So, SocMobilitat categorized the system as basic. However, the analysis of said commission contract, as well as the service provision contracts for the implementation and management phase of T-mobility, and the fact that the T-Mobility project involves the treatment of a high volume of personal data of people using the transport, which would include special categories of data, and that the system itself must provide critical services (interrelationship with users through the web portal, ticketing operation and data processing through the CPD, etc.) for the provision of a particularly relevant service such as a mobility service throughout the public transport network, leads to the conclusion that the categorization by SocMobilitat of the information system would require a higher level categorization , in accordance with the determinations of the National Security Scheme (ENS), and therefore, that the security measures that Indra had to apply in the execution of the contract have not been properly determined .

Fundamentals of law

1. The provisions of the LPAC , and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. The accused entity has made allegations both in the initiation agreement and in the resolution proposal, in this resolution all these allegations are analyzed.

2.1 On the lack of competence of the Authority in the categorization of the information system and in the determination of the applicable security measures.

In its allegations in the proposed resolution, SocMobilitat adds that the categorization of an information system in terms of security, and the consequent determination of the security measures to be adopted, is a competence that, in accordance with what is provided in articles 28 and 41 of Royal Decree 311/2022 by which the ENS is regulated (as well as articles 27 and 44 of the previous ENS- Royal Decree 3/2010), corresponds "exclusively" to the person in charge of treatment" (security manager), who has the necessary information to carry out said categorization, based on the importance of the information being processed in the system, the services provided and the effort of security required based on the risks to

which it is exposed (article 44 of the ENS), without the Authority having any competence to do so, nor having the necessary elements to carry out said assessment, running the risk , yes, this is how it is done, " *operating with presumptions and with judgments of inference, all of them contrary to the principles of legality and typicality."*

In this regard, it is worth saying that, effectively, it is the person in charge or the person in charge of the treatment, to whom it corresponds, or rather, who has the legal duty to categorize or assess in an appropriate way the level of risk presented by a system information and, on the basis of this assessment, determine the appropriate security measures to guarantee a level of security adequate to the risk of the data processing that is to be carried out, in compliance with the obligation established in article 32 of the RGPD.

Having said that, it should be noted that it is up to the Catalan Data Protection Authority, which is the body that is legally empowered to supervise the application of the RGPD and enforce it, to determine whether a non-compliance with the data protection regulations, and in the case that concerns us, in the exercise of the functions entrusted to him, and through the instruction of the corresponding sanctioning file where the reasons for its initiation have been fully justified (section of proven facts) and which form the basis of this resolution, has concluded that SocMobilitat has breached the obligation of article 32 of the RGPD, due to the fact that in the contract for processing orders signed with Indra on 09/30/2021 , for the provision of services in the implementation and management phase of T-mobility, SocMobilitat indicated to Indra that the categorization of the system was at a basic level (clause 7.5), which led to demanding the implementation of basic level security measures.

Thus, from the analysis of the above-mentioned data processor contract, as well as the service provision contracts for the T-mobility implementation and management phase signed between SocMobillitat and Indra , operating in file, it follows that the T-mobility project involves the processing of a high volume of personal data of people using transport, which includes special categories of data, and that the system itself must provide critical services (interrelationship with users in through the web portal, ticketing operation and data processing through the CPD, etc.), for the provision of a particularly relevant service such as a mobility service throughout the public transport network. The set of these concurrent circumstances in the processing of data, embodied in the conclusions of the report of the Technology and Security Area of the Authority, and reproduced in the section of imputed facts both of the agreement of initiation as of the resolution proposal, have not been refuted at any time by SocMobilitat , and are the ones that have led the Authority to conclude that the categorization of the information system as basic is not sufficient, in accordance with the determinations of the ENS, and that, therefore, SocMobilitat has not determined in an appropriate way in the commission contract, the security measures that Indra had to apply in the execution of the commissioned tasks.
This is why SocMobilitat 's statement that the Authority is not competent to determine that the categorization of the system as basic is insufficient in this case, and that this assessment would have been based on assumptions or insufficient evidence, is denied based on the considerations set out in this section.

2.2 On the lack of commission of the infringing conduct.

SocMobilitat reiterates in its allegations in the resolution proposal, as it did before the initiation agreement, that it has not committed the conduct that is imputed to it in the present procedure, that is to say, that it is not true that has not appropriately categorized the level of

risk for the data processing entrusted to Indra and, consequently, has not determined in an adequate way in the contract for the processing order, the security measures that Indra had to apply in the execution of the contract to guarantee a level of security appropriate to the risk, as long as:

- it is a proven fact that SocMobilitat carried out a risk analysis, as required by article 32.2 of the RGPD, and also the ATM (responsible for the treatment) in the order contract signed on 31/ 09/2021, risk analysis dated October 2020 and which SocMobilitat provided to the Authority in the framework of the actions of the PS (...), a different issue, SocMobilitat claims , is the assessment it makes the Authority in the present procedure, and which it does not share.

- that it is also a proven fact that SocMoblitat determined, clearly, the security measures that Indra had to adopt in the order contract, expressly referring to the need to apply the appropriate security measures to the National Security Scheme (BASIC LEVEL) as well as any other additional measures that were necessary to guarantee security in accordance with the risk, a matter which, according to him, did not raise any interpretive doubts in Indra .

That is to say, what SocMobilitat would come to support , is that through the risk analysis the possible deficiencies resulting from an inadequate categorization of the information system would have been "compensated".

In this regard, as was highlighted in the resolution proposal, the question is to what extent is compensable the fact that, as SocMobilitat maintains : " *They were established in the contracts of processing subcontractors with regard to the security of the treatment that these companies implemented the appropriate measures regarding the security of the treatment that corresponded to those of the Contracting Administration and that were in line with the National Security Scheme (Basic Level)"* . A compensation that SocMobilitat tries to attribute to the aforementioned risk analysis, or to the fact that despite the basic categorization "[...] *in any case, the person in charge had to implement mechanisms for:*

a. *Guarantee confidentiality , integrity , availability and resilience permanent of the treatment systems and services . _*
b. *Restore availability and access to personal data quickly , in the event of a fire physical or technical .*
c. *Verify, assess and value, in a rigid way, the effectiveness of the technical and organizational measures implemented to guarantee the safety of the treatment .*
d. *Pseudonymize and encrypt personal data , if applicable .*

In general, it had to adopt all those other measures that, taking into account the set of treatments it carries out, were necessary to guarantee a level of security appropriate to the risk. "

First of all, it should be stated that the categorization of the system provided for in the ENS must be the result of assessing the impact on the information and services that run on the information system under analysis - art. 43 and Annex I-. On the other hand, the risk analysis is the result of analyzing the risk derived from certain threats that are projected towards the most valuable assets of the system - measure op.pl.1-.

Consequently, while in system categorization the criticality of a certain information system is assessed (based on information and services), in risk analysis only the criticality of certain threats is analyzed in relation to the assets themselves that make up the system.

The fact that the scope of analysis is different is also transferred to the impact of the assessment. Thus, while the categorization of the system implies the establishment of a minimum level of security that crystallizes in all the security measures provided for in the ENS - annex II, the risk analysis only implies, for those cases in that it is considered that the risk of a certain element of the system is unacceptable, implement some specific measure that allows it to be moved below the maximum level of risk tolerance.

Thus, the system's own categorization affects the specific security measure "risk analysis" in such a way that an error in the categorization itself affects not only all the security measures but also the one corresponding to the risk analysis (op. pl.1).

The fact is that the risk analysis is configured as an additional or complementary element. A mere systematic observation of the legal norm already allows us to observe that while the categorization of the system constitutes the central and backbone of it constituting a chapter - the X- and the first of the annexes of the ENS, the risk analysis it is only one of the 75 measures foreseen in the ENS.

In short, the categorization of the system involves defining to what extent the system is critical and, based on the resulting category, determining which measures and to what degree must necessarily be applied, precisely in attention to the information and services linked to the system object of analysis. The practical implications of the establishment of this minimum therefore affect a significant number of different measures and in "how" they must be particularly applied, in accordance with the forecast made by the legislator.

The dysfunction associated therefore with an erroneous categorization of the system cannot be compensated either through a modulation, which will only include those indispensable measures to reduce an unacceptable risk of some "asset" of the system, nor with a mere generic reference to the need to guarantee the various dimensions of security, etc. And this because when the person in charge has to specify "what measures" he must necessarily apply and "how he must do it", the erroneous categorization will lead him to make mistakes, and to the effective non-application of measures that, in the framework of an adequate categorization of the system, would be mandatory.

Thus, as an example, in the contractual clause previously transcribed among the generic references, the following indication is found: " *b. Restore availability and access to personal data quickly, in the event of a physical or technical fire.* " Well, when the person in charge has to decide with a certain degree of precision which specific measures to apply, the unavoidable reference will be the erroneous categorization of the system (**basic)** that is contractually fixed.

The ENS foresees up to 15 measures that specifically affect "exclusively" availability (it should be borne in mind that many others also have an impact, although not only on the Availability dimension). Determining the level associated with the availability dimension is part of the information system categorization process. So much so that the fact that the information system is categorized as a basic category implies in turn that the maximum level relative to "Availability" is not higher than "low", which means that, eventually, only 3 of the 15 measures that the ENS envisages in relation specifically to "availability".

Finally, the own risk analysis referred to by SocMobilitat in its allegations and which it provided to the Authority, as has been said, within the framework of the PS (...) (incorporated into these actions as stated in the background 2 of this resolution), it also corroborates the fact that the analysis affects only a small range of security measures, so that it does not in any case make it possible to compensate for the minimum guaranteed when security measures security that derives from the categorization of the system (and from the correct assessment of the security levels corresponding to each of the dimensions that make up the process of categorizing the security system). Thus, it is only pointed out, and not very specifically, that it was necessary to carry out 6 actions / measures (p. 18), while the ENS lists 75. In addition, there are no guarantees that these 6 actions satisfy the requirements derived from the categorization that would eventually correspond. And, continuing with the previous example relating to "availability", it can be seen that through these 6 measures the shortcomings associated with the non-application or incorrect application of the 12 measures previously indicated would in no way be compensated.

In summary, the categorization of the system within the framework of the ENS is the main aspect in order to be able to determine the security measures that need to be applied, and subcategorizing the system has implications in terms of lack of protection that cannot be compensated neither in theory, nor in practice, nor through a risk analysis or a mere generic statement about, for example, the need to protect certain security dimensions; because precisely the objective pursued by the ENS is to specify the specific security measures that must necessarily be applied and how this application must be carried out in a specific way.

SocMobilitat 's claim cannot be successful , in the sense that through the risk analysis the possible deficiencies resulting from an inadequate categorization of the system would have been "compensated" 'information in the data processor contract signed with Indra , and that, therefore, the infringing conduct that is the object of imputation would not have been committed, which makes the following allegation also fall away.

2.3 On the absence of guilt and due diligence.

In line with the above, SocMobilitat asserts that, as long as it complied with the "requirements of article 32 of the RGPD" and "deployed a diligent activity at all times", from the moment when, according to in his opinion, he adequately assessed the level of risk for data processing involved in the execution of the assignment, and that, consequently, he determined in an adequate manner the security measures that the person in charge of the treatment had to 'implement, if the imputation made in the resolution proposal is maintained, SocMobilitat would be penalized for the materialization of an incident, (the incident suffered by Indra linked to the credentials of the configuration system of the portal access) and, therefore, by some results and not by the lack of determination of appropriate measures. In other words, he claims that data security would be considered to be an obligation of results and not of means, so the necessary element of guilt would be missing to be able to demand responsibility for the infringement that is imputed to him , as established by article 28 of Law 40/2015 on the Legal Regime of the Public Sector and the jurisprudence it invokes.

In this regard, it is necessary to highlight first of all that, indeed, it coincides with the accused entity in which the principle of culpability, that is to say, the need for there to be grief or guilt in the punitive action, is fully applicable to the law sanctioning administrative.

Now, in accordance with what has already been said repeatedly in this resolution, what is imputed to SocMobilitat in the present procedure is not the lack of adoption of basic level

measures in the configuration of the portal T-mobility's access that gave rise to the security incident reported for improper access, nor the fact that this incident materialized, but, as has also been said repeatedly, the fact that no having adequately assessed the level of risk for the processing of data derived from the technical services entrusted to Indra for the implementation and management of T-mobility, and from there not having determined adequately in the contract 'treatment order, the technical and organizational security measures that Indra had to adopt to guarantee a level of security adequate to the risk of the treatment that is the object of the order. And this infringing behavior has materialized, regardless of Indra's behavior , of the action of the third party that highlighted the vulnerability of the system, and of the same security incident caused by the lack of application on the part of 'Indra of the required basic level security measures.

So, based on all that has been said, and even if the conduct attributed to SocMobilitat could be due to a documentary error at the time of the configuration of the data processor contract, as it seemed to point out in the second allegation against the initiation agreement when it referred to an "erroneous document categorization" , a clear lack of diligence is observed due to the lack of verification of the obligations entrusted to the processing subcontractor in the contract regarding the data security.

This is the doctrine of the Supreme Court when it states, among others in the judgment of 25/01/2006 issued in matters of data protection, that " *the principle of culpability consists of the lack of diligence observed by the entity recurring when dealing in an automated way a data relative to the ideology of the complainant , resulting irrelevant the invocations that are made (...) about the absence of intentionality or the existence of the error, and it por cuanto the element culpabilístico of the sanctioning type applied attend when the expressed data on the ideology is included , the concurrence of a specific intentionality tending to reveal data is not required deprived of the affected* ".

In short, in order to determine the concurrence of the culpability element, it is not necessary that the facts have occurred with intent or intent, but rather " *the simple negligence or failure to comply with the duties that the Law requires the persons responsible for files or data processing to exercise extreme diligence* ... (Sentence of the National Court of 12/11/2010, appeal n. 761/2009), as is the case analyzed here, *where* it has been proven that there is a clear breach of Article 32 of the RGPD in the categorization of the level of security required in the processing of the data in question, attributable, at the very least, to a lack of diligence in fulfilling the obligations which in terms of security measures is imposed by the data protection regulations

And this 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 National Court in its judgment of 05/02/2014 (appeal n. 366/2012), when it maintains that the status of person responsible for processing personal data "imposes *a special duty of diligence when carry out the use or treatment of the data personal or su transfer to third parties , in what concerns the fulfillment of the duties that the legislation on data protection establishes to guarantee the rights fundamentals and freedoms people 's public physical , and especially his honor and personal and family intimacy , cuya intensity is enhanced by the relevance of the goods legal protected by those rules ".*

In conclusion, in the present case it is clear that the culpability element is present in the conduct of SocMobilitat , required by the regulations and jurisprudence to be able to demand

responsibility for the commission of the offense charged in the present sanctioning procedure, without his lack of intentionality affects this conclusion.

3 . In relation to the conduct described in the proven facts section, it is necessary to refer to article 32 of the RGPD repeatedly cited in this resolution, which provides for the following regarding the security of the 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 people físicas , the person in charge and the person in charge of the treatment they will apply measures technical and organizational appropriate to guarantee a level of security adequate to the risk , which may include , among others :
a) pseudonymization and data encryption personal ;
b) the ability to guarantee confidentiality , integrity , availability and resilience permanent treatment systems and services ; _ _
c) the ability to restore availability and access to data personnel quickly in the event of an incident physical or technical ;
d) a process of regular verification , evaluation and assessment of the effectiveness of the measures technical and organizational to guarantee the security of the treatment .

2. When evaluating the adequacy of the security level they will be particularly in account of the risks presented by data processing , in particular as a consequence of the accidental or unlawful destruction , loss or alteration of data personal transmitted , stored or treated in another way, or unauthorized communication or access to said data ."

Therefore, it is clear that article 32, with particular reference to section 2, establishes the obligation to carry out a risk assessment of the processing of personal data that is planned to be carried out, in order to be able to determine the appropriate security measures to guarantee their safety and the rights of the people affected.

Therefore, taking into account the state of the art, the costs of application and the nature, scope, context and purposes of the processing, as well as the risks of varying probability and severity to the rights and freedoms of natural persons, the person in charge and the person in charge of the treatment must establish or determine the appropriate technical and organizational measures to guarantee the level of security appropriate to the risk of the treatment.

In the case we are dealing with, it has been proven that in the treatment order contract signed between SocMobilitat and Indra on 09/30/2021 for the provision of services in the implementation and management phase of the T- mobility, on behalf of ATM, the entity SocMobilitat indicated to Indra that the security measures it had to implement for the provision of the services subject to the order were of a basic level (*The person in charge of the Tratamiento will implement the*
measures appropriate with respect to the security of the Treatment , which correspond to those of the contracting Administration and which conform to the National Security Scheme (***BASIC LEVEL*** *).(...)" (* clause 7.5) , that is to say, which was categorized the system as basic, when, in accordance with the concurrent circumstances in the treatment subject to the order, the basic level would not be sufficient, that is to say, that SocMobilitat did not adequately determine the security measures that the person in charge of treatment had to be

implemented for the provision subject to the order, which implies a breach of the provisions of article 32 of the RGPD.

This imputed fact, that is to say, the fact of not adequately determining the appropriate security measures to guarantee a level of security adequate to the risk, is constitutive of the infringement provided for in article 83.4.a) of the RGPD, which typifies as such the violation of *"the obligations of the manager and the manager pursuant to articles 8, 11, 25 to 39, 42 and 43"* , among which, those provided for in article 32 RGPD, the section 2 of which clearly links the correct determination of the security level of the treatment to the assessment of the risks it presents.

4 . By not fitting the entity SocMobilitat , in chief of the subjects provided for in article 77.1 of the LODGDD , 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, the amount of the administrative fine to be imposed must be determined. According to what is established in articles 83.2 RGPD and 76.2 LOPDGDD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the investigating person in the resolution proposal, the sanction should be imposed of 10,000 euros (ten 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 lack of intentionality (art.83.2.b) RGPD).
– The lack of commission of previous infringements (art.83.2.e) of the RGPD), since it is not known that SocMobilitat has previously been sanctioned for a violation of data protection regulations.
– The lack of proof of obtaining benefits as a result of the infringement (art. 83. 2. k) RGPD and 76.2. c) LOPDGDD).

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

– The nature, gravity and duration of the infringement (art.83.2.a).
– SocMobilitat 's activity with the processing of personal data, as SocMobilitat is the company tasked by Barcelona's ATM to develop and implement contactless payment technology in public transport the scope of the integrated tariff system, and the integration of other mobility systems in the future.

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

By virtue of this power, SocMobilitat should be required to adopt the corrective measure consisting of urging to Indra , based on an adequate categorization of the risk of the information system, to the adoption of the appropriate security measures to guarantee a level of security appropriate to the risk for the provision that is the object of the order, in accordance with what establish articles 28 and 32 of the RGPD, given that the measures corresponding to the basic level of the ENS are insufficient.

Once the corrective measure described has been adopted in the period indicated, within the next 10 days SocMobilitat must inform the Authority, without prejudice to the Authority's inspection powers to carry out the corresponding checks .

For all this, I resolve:

1. To impose on SocMobilitat the sanction consisting of a fine of 10,000.- euros (ten thousand euros), as responsible for an infringement provided for in article 83.4.a) in relation to article 32.2, both of the RGPD.

2. Require SocMobilitat to adopt the corrective measure indicated in the 5th legal basis and certify to this Authority the actions taken to comply with it.

3 . Notify this resolution to SocMobilitat .

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.