File identification

Resolution of sanctioning procedure no. PS 35/2022, referring to Indra Sistemas, SA.

Background

1 . On dates 05/10/2021, 06/10/2021, 07/10/2021, and 26/10/2021 the Catalan Data Protection Authority received up to six complaints (two of them for referral of the Spanish Data Protection Agency) filed separately by citizens against the Metropolitan Transport Authority (henceforth, the ATM), and a complaint filed against Societat Catalana per la Mobilitat, SA, (in hereafter, SocMobilitat), due to an alleged breach of the regulations on personal data protection.

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 (name and surname, DNI, postal address and email). 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 the following documentation:

-Screenshot of the tweet thread published by a citizen on 05/10/2021 (at 3:39 p.m.) showing the security loophole and the way in which third-party information could be accessed, and indicated the steps to follow (https://twitter.com (...)).

-News published in the media on 10/05/2021 " *An error on the T-Mobilitat website exposes user data".*

- Tweets published by T-Mobilitat on its channel on 10/05/2021 and 10/06/2021, respectively, in relation to the reported incident:

" *We have detected an operational error on the T-Mobilitat website, in the testing stage. The bug allowed access to non-sensitive data for a limited time. The ATM will open an information file on the company responsible for this web development* " (10/05/2021 at 5:00 p.m.).

Access to the T-mobilitat.cat website in this test phase has been temporarily suspended . We have decided to carry out, with the Cybersecurity Agency, an exhaustive analysis to rule out any other undetected vulnerabilities ." (06/10/2021 at 6:00 p.m.).

2. The Authority opened a preliminary information phase, in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat , and article 55.2 of Law 39/2015, of October 1, of the common administrative procedure of public administrations (from now on, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure, and the persons allegedly responsible.

3. 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 movement 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.

4. In the prior information phase, on 11/15/2021 the ATM was required to comply with the following:

- On the one hand, to inform if new information was available that would modify in some aspect the statements made, as part of the notification to the Authority of the security breach, in relation to the result of the analysis on the incident carried out by the Cybersecurity Agency, and included in "the report on the security vulnerability detected on the T-mobilitat.atm.cat portal on 10/05/2021", and in its annex, and specifically regarding :

"Chronology of the incident
On October 5, 2021 at 3:39 p.m., a citizen posts on Twitter a vulnerability detected on the T-mobilitat.atm.cat portal
At 16:24 ATM indicates the vulnerability to the SOC provider Mobilitat.
An urgent technical committee is convened to review it and proceed with its mitigation.
At 16:40 the vulnerability is mitigated.

"Access to data
The compromised data is the first name, last name and user ID, not the password to enter the web portal. Emphasize that there was no impact on the data located in the Central Systems of the T-mobility system but only on those corresponding to the web portal. There has also been no impact on the integrity of the data.
The extent of the compromised data has been confirmed by the Cybersecurity Agency of Catalonia as a conclusion of the data analysis they have carried out based on the information provided by ATM (See Annex 1).
The volume of compromised data is 2,161 records, of which 1,046 are internal to the system test.

Cause of vulnerability
In the Liferay technology infrastructure of the T-mobilitat.atm.cat portal, the user, password, and the native possibility to enter, which comes by default from the manufacturer, had been configured.
In this way, the configuration pages of the portal itself could be accessed from the Internet and entered with the default user.

Mitigation actions carried out
The following actions have been carried out on the Liferay technology infrastructure of the T-mobilitat.atm.cat portal:
• *Leave only one administrator user and change his password.*
• *Disconnect the native ability to enter Liferay .*

• *Check through a script that no portal content has been modified. In this case it has been confirmed that there has been no modification."*

- On the other hand, to confirm whether the data security breach suffered would have occurred within the framework of an assignment entrusted to the Catalan Society for Mobility, SA. In the event of an affirmative answer, provide a copy of the data processor contract signed with said entity.

5. On 22/11/2021, the ATM responded to the previous request, through a letter in which it set out the following:

- That there had been no modification, regarding the information provided in the notification of the security breach, which "was correct and conformed to the reality of the events that occurred."

- That the security breach occurred "within the framework of an assignment entrusted to the Catalan Society for Mobility SA. "

Attached was the contract for ordering the treatment signed between the ATM (responsible for the treatment) and SocMobilitat (responsible for the treatment) on 30/09/2021 for the provision of services for the implementation and management phase of T-Mobility.

6 . In accordance with the antecedents that have been related so far and with the result of the investigative actions carried out in the framework of the previous information, which includes both the complaints filed against the ATM (to which assigned no. IP 394/2021, 395/2021, 400/2021, 403/2021, 431/2021 and 432/2021) as the complaint lodged against Soc Mobilitat (to which assigned no. IP 397/2021), the Director of this Authority agreed on 10/01/2022 to initiate disciplinary proceedings against the data controller Soc Mobilitat (PS (...)), for the alleged violation of the principle of data security in the deployment of the T-Mobilitat portal and consequent violation of its confidentiality, and in accordance with the regime of responsibility in the matter of data protection provided for in article 28.10 of the RGPD, which provides that the person in charge of the treatment is responsible to the control authority, of alleged violations of the data protection regulations that may be committed in the development of the order that do not comply with what is established in the order. This initiation agreement was notified to the imputed entity on 01/17/2022.

7. On 04/02/2022, SocMobilitat made objections to the initiation agreement, providing various documentation along with its written statement. Among this documentation, the data processor contract signed between SocMobilitat and Indra Sistemas SA (hereinafter, Indra), on 09/30/2021 for the provision of technical services within the framework of the T-mobility Technology Project awarded to SocMobilitat (document no. 2), among which, and as stated, the deployment of the T-mobility portal, and the "Legal report in relation to the security breach of the extranet portal of T-Mobilitat" (document no. 6).

8 . In view of the allegations made, and the analysis of the documentation provided by the accused entity, on 04/26/2022 SocMobilitat was required to provide additional documentation, more specifically:

-Copy of the service provision contracts for the implementation and management phase for T-Mobilitat signed between SocMobilitat and Indra on 07/21/2014, and of their subsequent

modifications or addenda, to which it referred the data processor contract signed between SocMobilitat and Indra on 30/09/2021 (clause 2a: "Conditions and purposes of treatment" :

> *" 2. Conditions and purposes of the treatment*
> *2.1 "The treatment will consist of the technical services within the T-Mobility Technology Project attributed and assumed by INDRA in the Service Provision contracts for the implementation phase for T-Mobility and in the Service Provision for the phase management agreement for T-Mobilitat signed between SOC MOBILITAT and INDRA on July 21, 2014 and its subsequent amendments and additions."*

-Copy of the assessment or risk analysis carried out by SocMobilitat regarding the processing of data derived from the technical services entrusted to Indra in said contracts. In this regard, the data controller contract stated the following:

> "7. Obligations of the data controller (...)
> *"7.5. Safety of Treatment*
> *The person in charge of the treatment will implement the appropriate measures regarding the security of the treatment, which correspond to those of the contracting administration and which are in line with the National Security Scheme (BASIC LEVEL)." (...).*

9 . On 05/03/2022 the entity SocMobilitat complied with said request and provided a copy of the service provision contracts for the implementation and management of T-Mobility signed between SocMobilitat and Indra on 07/21/2014 and of its modifications, and a copy of the risk analysis.

In said service provision contracts for the implementation and management of T-Mobility signed between SocMobilitat and Indra on 21/07/2014, the task assigned to Indra is the deployment of the T-mobility web portal.

10 . From the analysis of all the documentation provided by SocMobilitat in the processing of the sanctioning procedure (...), it was found that the facts that motivated its initiation, that is, the violation of the principle of data security in the deployment of the T-Mobilitat portal and consequent violation of its confidentiality, due to lack of application of certain security measures, was attributable to Indra Sistemas, SA within the framework of the contract for the processing of personal data signed between SocMobilitat (awardee of the contract and in charge of the treatment) and Indra (shareholder of SocMobilitat and sub-in charge of the treatment), for the provision of services in the implementation phase and management of T-mobility.

In this regard, the contract for the processing of personal data signed between SocMobilitat and Indra on 30/09/2021 stipulated the security measures that Indra had to adopt for the service subject to the order:

"7. Obligations of the data controller (...)

"7.5. Safety of Treatment
The person in charge of the treatment will implement the appropriate measures 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 the confidentiality, integrity, availability and permanent resilience of the Treatment systems and services.
b. Quickly restore availability and access to Personal Data in the event of a physical or technical incident.
c. Verify, evaluate and assess regularly, the effectiveness of the technical and organizational measures implemented to guarantee the safety of the treatment.
d. Pseudonymize and encrypt personal data, if applicable.

Together, it must adopt all those other measures that, taking into account the set of treatments it carries out, are necessary to guarantee a level of security adequate to the risk." (...).

Having said that, the security measures that were violated in the configuration of the T-mobility portal, which led to the access being open, and in turn, accessible to third parties, are of a basic level (section 4.1.2 "Security Architecture"), 4.2 relating to access control, and section 4.3.2 relating to "security configuration") of the National Security Scheme (ENS) approved by Royal Decree 3/2010, to which it is referred to.

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 agreed to postpone procedure no. (...) initiated against SocMobilitat, considering that responsibility could not be attributed to SocMobilitat for the lack of application of the appropriate technical measures to guarantee the security of the data subject to treatment, given that the adoption of these security measures, and specifically those of a basic level, was an obligation that corresponded to Indra, as sub-processor, as stipulated in the contract for the processing of personal data signed on 30/09/ 2021 between SocMobilitat and Indra. In the same dismissal resolution, it was agreed to initiate a disciplinary proceeding against Indra Sistemas, SA, in order to determine its alleged responsibility for the lack of application of basic level technical measures in the implementation of the T-mobility web portal, required by SocMobilitat, which enabled third parties to access the personal data of users recorded there.

In this sense, it should be borne in mind that the data protection liability regime established in article 28.10 of the RGPD, to which reference has been made before, is also applicable to the sub-processor, in accordance with the provisions of article 28.4 of the RGPD and 70.1.b) LOPDGDD (which is considered, in any case, a person in charge of the person in charge of the treatment), and, therefore, is also responsible, before the authority of control, of the alleged violations of the data protection regulations that may be committed in the development of the assignment that do not comply with what is established in the assignment.

11. On 01/06/2022, by the Agreement of the director of the Catalan Data Protection Authority, the present sanctioning procedure against Indra was initiated, for an alleged infringement provided for in article 83. 4 .a), in relation to article 32.1; all of them from the RGPD. This initiation agreement was notified to the imputed entity on 02/06/2022.

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.

12. On 15/06/2022, Indra filed objections to the initiation agreement .

13 . On 09/09/2022, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority impose a fine of 25,000 euros on Indra as responsible, 'an infringement provided for in article 83.4.a) in relation to article 32.1, regarding the principle of data security, both of the RGPD.

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

14. On 09/22/2022, 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 in the implementation and management phase of T-mobility (among others, the deployment of the T-mobility portal).

The execution of this contract involved Indra accessing and managing the personal data of T-Mobilitat users, and it was required to adopt basic ENS measures.

In the framework of this assignment, the data processor, Indra, did not apply the basic technical security measures required by SocMobilitat, given that when configuring access control to the T-Mobilitat web portal, it was not modified the password that by default the manufacturer of the "Liferay" technology infrastructure assigns to the administrator (public access credential), in such a way that the access was open, and in turn, accessible to third parties, insofar as the 'ENS requires for basic level categorized systems.

So, from the launch of the T-Mobilitat portal (at 08:00 on 04/10/2021), until 16:40 on 05/10/2021, anyone could access through from the internet to the configuration pages of the T-mobilitat web portal, and to the personal information of third parties contained there, as well as to modify it, if the password or password assigned by default by the manufacturer of the infrastructure of "Liferay" technology (software used to manage t-Mobilitat cards) to the administrator. Specifically, the personal data of the users accessed were: first and last name, user ID, and the fact that they had applied for the new T-Mobility card.

Thus, access by a third party to said data on 05/10/2021 at 3:39 p.m. (citizen/user of the portal who published the tweet) is certified.

Fundamentals of law

1. The provisions of Law 39/2015, of October 1, on the common administrative procedure of public administrations (the LPAC) , and article 15 of Decree 278/1993, in accordance with the DT 2a of Law 32/2010, of October 1, of the Catalan Data Protection Authority. The

resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority , in accordance with articles 5 and 8 of Law 32/2010.

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

2.1. About the accessibility of the system by third parties.

Indra asserts that it acknowledges that when configuring the access control to the T-Mobility web portal, it did not modify the password that by default the manufacturer of the "Liferay" technology infrastructure assigns to the administrator, but it denies that this was which caused that, from the launch of the T-mobility portal until 4:40 p.m. on 05/10/2021, access to the portal remained open, and that anyone could access it via the internet to the information recorded there.

In this sense, Indra defends, as it already stated in the allegations in the initiation agreement, that from the moment the web portal was launched, it had implemented a user identification and authentication system protected with credentials, and that while it is true that access had been configured with the native possibility of entering with the credentials that come by default from the manufacturer, these credentials were under the exclusive control of the administrator user, and it reiterates that what caused them to cease to be under its exclusive control was the malicious action of a third party that, taking advantage of its computer knowledge, violated the security measures implemented by Indra, and through penetration tests not authorized guessed the password, accessed ATM's reserved data, and made the administrator's credentials public through social media, at which point the credentials were no longer under control exclusive to the administrator user, and access to the system was left open.

In this regard, that is to say, as will be analyzed in detail in the next allegation and as was already highlighted in the proposed resolution, that it cannot be admitted that the identification and authentication system implemented by Indra was protected with credentials that were under the exclusive control of the administrator, and that what caused the entry door to the system to be open was the action of a third party who violated said system, considering that it is a fact undisputed that, through oversight or error, the standard password assigned by default by the manufacturer to the administrator (extreme, it is insisted, acknowledged by Indra) had been left on (or not removed), such that anyone could enter with said password, without, therefore, the administrator having at any time "exclusive control" over said password, as Indra maintains, because it is clear that from the moment when these were of a public nature (published in the manufacturer's technical documentation and accessible on the internet by anyone), the administrator had no control over them.

That is why the allegation put forward by Indra cannot prosper in the sense that what caused the access to be open and accessible to third parties, was the violation of the basic level measures implemented by Indra, as that it cannot be maintained that he had implemented said measures, when the access control system did not have a system of authentication of users protected with credentials configured by the administrator himself, in order to guarantee that they could only access the data the authorized persons.

Finally, it should be remembered that, as was already made clear by the instructing person in the resolution proposal, the charge against Indra in the present procedure does not derive

from the fact that access to the data has materialized by part of an unauthorized third party, but that the conduct that is imputed to him is not having implemented the corresponding security measures in the configuration of the access control to the web portal to guarantee the confidentiality of the data recorded there and to ensure its protection against improper access attempts, and specifically measures at the basic level of the ENS that were expressly required by SocMobilitat in the order contract signed on 09/30/2021.

2.2. On Indra's breach of security measures.

2.2.1 The duty to preserve confidentiality by implementing appropriate technical measures.

The allegations made by Indra focus exclusively on discussing the application of the security measures corresponding to the ENS, and omits any reference to the obligations that are required directly from the RGPD, the central axis of the whole of the data protection regulations, more specifically, the obligation to maintain the confidentiality of the personal data being processed, which is a duty set out as a guiding principle in article 5.1 f) of the RGPD, constantly invoked both in the initiation agreement and in the proposed resolution, and which imposes that the data must be:

> " *treated in such a way as to guarantee an adequate security of personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality »)* "

This obligation is reinforced in art. 32.1 of the RGPD, the breach of which is imputed in the present procedure:

> " *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 if applicable includes, among others:*
>
> *b) the ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems and services (...)* ".

In relation to this obligation, it is not a question that is under discussion, that the obligation to guarantee the confidentiality of personal data through the application of appropriate security measures , was expressly included in the contract of the person in charge of the treatment signed between SocMobilitat and Indra, i.e. Indra, had to implement the security measures corresponding to the basic level of the ENS, and carry out the necessary actions to guarantee at all times the confidentiality of the information processed, which it did not, as discussed in the following subsections. Nor is it debatable that changing the default password in the "Liferay" management software does not mean going beyond the current state of the art nor does it involve significant implementation costs.

In this framework, the object of the ENS is precisely to "ensure the access, **integrity** , availability, authenticity, **confidentiality,** traceability and conservation of the data, information and services used in electronic media that they manage in the exercise of their competences ". (art. 1.2).

Having made these considerations in advance, the arguments put forward by Indra are analyzed below to try to justify that, in the configuration of the access control to the T-mobility web portal, it complied with the required basic level security measures by SocMobilitat.

2.2.2 The duty that access control is effective through the use of secret keys (passwords).

One of Indra's main allegations, as already mentioned in point 2.1 of this resolution, is to ensure that it had an adequate access control system since "None of *these rules* [previously cites a following of norms of antecedents and contemporaries in the ENS] *expressly establishes what is meant by protecting the system so that no one accesses the resources without authorization, besides citing the need to configure an authentication system based, for example, on username and password* [...]".

However, when, as Indra acknowledges, reference is being made to the need for the access system to be based on the combination of user and password, the nature of the protection required is already being specified. Well, "password" implies, according to the definition of the RAE, "a ***secret*** *password that allows access to something, someone or a group of* ***previously inaccessible people*** ".

In fact, this same secret character is also established on page 4 " Guide to ICT Security CCN-STIC 821. Appendix V: Rules for creating and using passwords NP40": "It *is especially important to maintain the secret character of the password It must not be given or communicated to anyone. In case of having had the need to do so, the user must proceed to change it immediately* . It is a particularly valid instrument as a means of interpreting the ENS, given that the technical instructions of the CCN-STIC are expressly provided for this purpose in the ENS itself (section 7 of Annex II).

In other words, in order for an authentication system to be considered minimally effective as a protection, it must require a user and a password understood as secret information. Therefore, in no case could the system implemented by Indra be considered valid to the extent that it did not comply with something essential such as that the password be secret, since being the one incorporated by default by the manufacturer it was publicly accessible.

Measure 4.1.2 "Security architecture [op.pl.2]" of the ENS indicates that also for basic category systems it will be necessary to detail a user identification and authentication system, and measure 4.2 "Control of access [op.acc]" details the indispensable features of both identification [op.acc.1] and authentication [op.acc.5]; both measures (4.1.2 and 4.2), expressly mentioned in the initiation agreement and the resolution proposal.

The factual imputation to Indra consists precisely of having omitted the duty to change the password that the manufacturer set by default in the Liferay functionality. Consequently, everything that specifically refers to user authentication is particularly transcendent and clarifying.

Certainly, measure "4.1.2 Security architecture [op.pl.2]" establishes different options for the identification and authentication of users, including "passwords". In any case, if you opt for the option of using passwords , it is inherent in the same concept, as explained, that it has a "secret" character; characteristic that, as is obvious, is not complied with if it is a password that a certain manufacturer incorporates by default in its solutions, because that password is

known by multiple clients of the same solution and can even, as in this case case, having been made public via the internet.

Section 4.2.5 which deals specifically with authentication also reinforces the conclusion that the maintenance (not change) of a password that is found in a technological solution by default by the manufacturer breaches the ENS. And it is that whatever option is used for user authentication, it must be complied with in order to guarantee its "security" that (i) " ***1. The credentials will be activated once they are under the effective user control*** ", and (ii) ***Credentials will be under the exclusive control of the user. "*** Neither of these two inexcusable requirements are satisfied, it is insisted, if we are dealing with passwords that by default had been implemented by the manufacturer of the corresponding technological solution, because the credentials are at no time under the exclusive control of the user in the since it is a key known to third parties (other purchasers of the solution, the producer of the same, whoever has access to it via the internet, etc.).

In simpler terms, the RGPD itself and, to a greater degree of concreteness the ENS, what they establish is that - among other dimensions - the confidentiality of information must be protected. This is mainly achieved by establishing access mechanisms (door) in such a way that only those who are authorized to do so (who have the key to open the door) can access the information. This protection mechanism would become ineffective if these keys were known to everyone (manufacturer, Internet users, other buyers of the solution, etc.). It is clear that neither the RGPD nor the ENS can draw the conclusion that a situation like the one described can be valid, given that it would directly confront the purpose of protecting confidentiality and, moreover, it would go against the that when the authentication measures are particularly defined it is required: passwords as something intrinsically secret and, therefore, of "exclusive" control by the user. Requiring to place a door that could be opened by anyone would not make any practical sense beyond generating a mere appearance of security when it is non-existent.

In summary, the use of a password as a means of authentication requires that the information used be "secret" since it is an inherent property, because if the password is known, the requirement that this information/key be under the exclusive control of the user.

2.2.3 The comprehensive application of the obligation to establish effective access control.

The last of the allegations put forward by Indra in order to try to maintain that it would not have breached the required basic level security measures, consists in pointing out that the obligation that the password be secret and under the exclusive control of the user would not apply to the extent that: (i) it would only be provided for the "equipment" and that, (ii) taking into account - in his opinion - that the equipment does not have software, this obligation would not apply to the subject matter of the file since Liferay is software.

With a preliminary character, it is necessary to contextualize that, as already explained, the obligation to protect confidentiality is projected for all data protection treatments under the RGPD and, consequently, it does not depend on which element specific technician is used to carry out the treatment. Similarly, the measures indicated by the ENS (4.1.2 and 4.2 - and singularly 4.2.5.-) consistently refer to the entire information system and its own resources:

> 4.1.2 " *The Security of the system will be subject to a comprehensive approach detailing, at least, the following aspects* [...]"

> 4.2 " *Access control covers the set of preparatory and executive activities so that a certain entity, user or process can, or cannot, access a system resource to perform a certain action* "
>
> 4.2.5 " *The authentication mechanisms against the system* [...]"

It is noted that these requirements are not likely to be altered depending on the specific nature of which specific element is used. In fact, taking into account that Indra assumes that Liferay is in any case a component of the system (p.10 of the allegations in the initiation agreement), measures 4.1.2 and 4.2 - and singularly 4.2. 5- they would undoubtedly apply to him. Rather, precisely in relation to the "components of the system, section 4.2.2 Access requirements [op.acc.2] reinforces the importance of controlling access precisely to the different components of the system (section c):

> c *) In particular, access to the system components and their configuration files or records will be controlled.* "

Consequently, this allegation cannot detract from the considerations set out in the previous two subsections. And this because Liferay is part of the system, which the ENS itself is responsible for defining in its Annex IV as the " *Organized set of resources so that information can be collected, stored, processed or treated, maintained, used, shared, distribute, make available, present or transmit* ." In other words, when the indicated measures refer to the protection of the information system, it involves securing the set of resources that are used to carry out the processing of the information, including the software (Liferay).

In other words, it is incorrect to state that the change of passwords only affects a specific type of "equipment", when the protection of information has a vocation to be comprehensive in the sense that the protection of the system as a whole happens, obviously, to ensure the set of elements that make it up (one of which, according to Indra, is the software) and, as explained in the two previous subsections, the protection of confidentiality, and the specific obligations of the ENS , necessarily involve changing the passwords that may have been installed by default by the manufacturer .

In short, the imputation of the infringement to Indra of breaching the data protection regulations neither incurs nor can do so in an extensive interpretation of any specific concept, since the obligation that passwords be secret and under the control of the user does not have any dependence on which element is involved (hardware or software...), only that it is part of the system that processes the information.

Despite the fact that responding to the rest of the allegations made by Indra would not be necessary based on the previous consideration, it is considered appropriate to do so with a spirit, again, of completeness and, also, to demonstrate the incorrectness of his approach.

Thus, Indra points out that it is necessary to make a separation between equipment and software, placing them as antagonistic concepts. Nothing could be further from the truth. The RAE defines "equipment" as "a set of devices consisting of a computer and its peripherals" and "[electronic] computer" as "an electronic machine that, through certain programs, allows storing and processing information and solving problems of various kinds" .

That is to say, again, it states that it is inherent in "equipment" that there are programs so that IT/electronic functions linked to data processing can be carried out.

The same conclusion is reached by analyzing the measure itself pointed out in the framework of this file "4.3.2 Security Configuration [op.exp.2]", consisting in the obligation to remove the standard passwords of the "equipment " prior to its entry into production. Well, the very existence of a password in a computer environment, as is the case, implies the presence of a software that makes it possible to accurately check whether the entered password is valid or not.

So, the basic error of a technical nature in Indra's allegation also leads to the unduly reductionist interpretation he tries to make losing any meaning, not only structurally (Liferay is an element of the system), but also material (it is not possible to contrast software with equipment since software constitutes an essential aspect of any computer equipment).

Returning to the beginning of this subsection, even in the mistaken case that someone considers that "equipment" is something antagonistic to "software", it must be remembered that Indra assumes that the software in any case is a "component of the system", such so that the obligations established at system level are, without any doubt, applicable. Thus, when the RGPD and the ENS (art. 1.2) require that the confidentiality of information be protected and when the ENS specifies that it is necessary to establish access control at systems level (4.2.op.acc) it is it is clear that such obligation is also projected towards the Liferay program.

From a material point of view, defending the opposite is equivalent to maintaining that confidentiality is adequately preserved even if the passwords to access the software as an administrator - and therefore to be able to make the most significant changes - are known by manufacturers, other buyers and by Internet users in general.

And, from a legal point of view, assuming the position of Indra c would contravene the very spirit and ultimate functionality of the rule as well as multiple precepts such as those indicated and even others that include this same spirit: access protection remote [op.acc.7] *"that no one will access resources without authorization.* "

In short, each and every one of the specific measures referred to in the instruction of this file are of a "basic" nature, and were required of Indra, bearing in mind that the order contract signed with SocMobilitat stated expressly the obligation to implement in any case the security measures that correspond to a basic category system.

2.3 On the absence of guilt.

Along the lines of the above, Indra argues that if the imputation made in the resolution proposal is upheld, Indra would be sanctioned for the materialization of improper access by a third party, and not for the lack of application of security measures, that is to say, it would be considered that the security of the data is an obligation of results and not of means, so the necessary element of guilt would be lacking in his conduct to be able to demand responsibilities in the offense imputed to him, as provided in 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, the data security violation behavior attributed to Indra is, precisely, the lack of implementation of required security barriers by SocMobilitat in order to protect the confidentiality of the data recorded on the portal web, and it is an undisputed fact that the system went into production with real user data, leaving the manufacturer's default credentials enabled.

Therefore, it is clear that insofar as Indra did not implement basic level security measures that were required of it, in its capacity as sub-processor, it breached the obligation established in Article 32.1 of the RGPD to protect the security of the data, and this is undoubtedly an obligation of the media, being therefore responsible for the infringement that is imputed to it in this procedure, because its commission materialized independently of the actions carried out by the third party to access to the processed data. In other words, the commission of the infringement would also be imputable to Indra even if the improper access by this third party had not occurred.

In summary, the target element of the infringing type of Article 83.4.a) of the RGPD, is perfected from the moment the system entered the production phase and did not implement necessary technical and organizational measures that guarantee the security of personal data and prevent their alteration, loss, treatment or unauthorized access, and more specifically basic level measures, in accordance with the provisions of the aforementioned article 32.1 of the GDPR and the contract that stipulated Indra's obligations.

And his argument that the system was in a testing environment, and that he was responsible or in charge of processing, but in no case Indra, who ordered it to go into production, is also not admissible. And this because it was a test environment carried out by Indra with real user data that was exposed on the internet (extranet portal), and software tests with personal data also constitute treatment subject to the obligations established the RGPD and, obviously, also those established in article 32.1 of the RGPD regarding data security.

In summary, Indra had the duty to comply with the security obligations stipulated in the contract signed with SocMobilitat and to act with the necessary diligence so that the security of personal data was not compromised, guaranteeing that they only accessed the processed data authorized persons, which required it to establish a mechanism that would allow the unequivocal and personalized identification of any user who tried to access the information system, circumstances that were not met in the present case, in which, whether due to negligence or due to "an operational error", as was said in the Tweets published by T-Mobilitat on its channel on 05/10/2021 and 06/10/2021 (1st precedent), the public password was not changed defect assigns the manufacturer to the administrator, in the testing phase of the implementation of the T-mobility card, which led to an open door to the information contained in the platform.

In this respect it is necessary to refer to the jurisprudential doctrine which maintains that it is not necessary to have a willful conduct on the part of the offender, but rather "the simple negligence or failure to fulfill the duties that the Law imposes on the persons responsible for files or the treatment of datos de extremar la diligencia..." (Judgment of the National Court of 12/11/2010, appeal n. 761/2009).

Along the same lines, the Supreme Court pronounces itself, among others, in the judgment of 01/25/2006, also issued in the area of data protection, when it states that "the principle of culpability consists in the lack of diligence observed by the appellant entity when processing

data related to the ideology of the complainant in an automated manner, rendering irrelevant the invocations that are made (...) about the absence of intentionality or the existence of the error, and this because of the culpable element of the sanctioning type applied occurs when the expressed data on the ideology is included, not being necessary the occurrence of a specific intention tending to reveal private data of the affected".

In short, in order to determine the concurrence of the culpable element, it is not necessary that the infringing acts have occurred with intent or intent, but it is sufficient that there has been negligence or a lack of diligence in the fulfillment of the obligations that they are legally enforceable, as would be the case analyzed here, in which he did not even implement basic security measures that had been specifically contractually required of him. And, it is worth saying, 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 Judgment of the National Court of 02/05/2014 (appeal n. 366/2012) issued in the matter of data protection, which maintains that the status of person responsible for 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 natural persons, and especially their honor and personal and family privacy, whose intensity is enhanced by the relevance of the legal assets protected by those rules."

In the present case, the lack of diligence is evident in the face of the undisputed fact that access to the web portal was left configured with the password that comes by default from the manufacturer when real user data was being processed, which constitutes a clear breach of his obligations regarding the security measures he had the duty to implement, and which is imputable to Indra , even though it derives from a human error of a worker, in accordance with the system of responsibility provided for in the RGPD, and particularly in article 70 of the LOPDGDD, in which it is established that responsibility for breaches of the data protection regulations falls, among others, on those responsible, or in his case, about those in charge of the treatments, and not about their staff.

In conclusion, in the present case it is clear that the culpability element is present in Indra's conduct, required by the regulations and jurisprudence to be able to demand responsibility for the commission of the offense charged in the present sanctioning procedure, given his lack of diligence in fulfilling the obligations that were due to him.

2.4 On the adoption of immediate measures.

In this regard, Indra asserts that once it became aware of the vulnerability, which was published at 3:39 p.m. on the same day 05/10/2021 on social networks, it proceeded immediately to resolve the incident.

In this sense, Indra highlights that in just 61 minutes since it became aware of the data leak, it blocked "any access by unauthorized third parties", and carried out the following actions on the infrastructure of Liferay technology of the T-mobility portal, in order to mitigate the possible adverse consequences for the people affected, and eliminate the risks of new access, and specifically:

• Only one admin user was left and his password was changed.

• The native ability to enter “Liferay” was disconnected.
• An audit of "Liferay" content management analyzes was carried out, to verify the total content of the portal and order them by date of modification. " *In this way it was possible to certify that during the period of time in which the portal was accessed as an administrator until the incidence was mitigated, no modification was made to any content.*

In this regard, it must be emphasized that the actions carried out by Indra immediately and as soon as he became aware of the incident, do not allow the infringement charged against him for the violation of the security of data, although they are taken into account as a mitigating circumstance in the quantification of the penalty, in accordance with the analysis carried out in the 5th legal basis of this resolution, and they display effects as far as the fact that in the present procedure should not require the adoption of corrective measures to correct the effects of the offense committed.

2.5 On the lack of damages.

Finally, in the conclusions section, and as the last allegation in order to justify its request for the suspension of the procedure, Indra asserts that the security incident that occurred would not have had negative consequences for the people affected, that is to say that no damages would have been generated.

In this regard, it must be said that among the objective elements that make up the infringing type provided for in article 83.4.a) of the RGPD is not included the need for the person holding the data, in relation to which after the infringement has occurred, consider your privacy or privacy violated. The type only requires , as has been said, the lack of adoption of technical and organizational measures to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of the RGPD.

In any case, it should be remembered that in the present disciplinary file there are up to seven complaints from people who have understood that the privacy of their data has been violated as a result of the infringement attributable to Indra.

For everything that has been explained so far, the allegations made by the entity imputed to the proposed resolution cannot be successful.

3 . In relation to the conduct described in the proven facts section, relating to the lack of application of the basic level security measures required to guarantee a level of security adequate to the risk, it is necessary to go, as has been said, to article 32.1 of the RGPD, which provides that:

"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 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, which if applicable 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."

As has also been said, with respect to the conduct described in the proven facts, it is considered that Indra has violated security measures, at a basic level, of the National Security Scheme (ENS) approved by Royal Decree 3/2010, and applicable to Indra, in accordance with the first additional provision of the LOPDGDD (Security measures in the field of the public sector), due to the order contract signed with SocMobilitat, which were required of him in said contract. And specifically, the measures detailed below were violated:

1. Section 4.1.2 *"Security Architecture"* of Annex II ("Security Measures") of the ENS, determines the following:

The security of the system will be the subject of a comprehensive approach detailing, at least, the following aspects:
BASIC category
a) (…)
d) User identification and authentication system:

1. Use of agreed keys, passwords, identification cards, biometrics, or others of a similar nature.
(...)

2. Section 4.2 relating to access control determines the following:

"Access control covers the set of preparatory and executive activities so that a certain entity, user or process, may or may not access a system resource to perform a certain action.

The access control implemented in a real system will be a point of balance between ease of use and information protection. In low-level systems, comfort will be prioritized, while in high-level systems, protection will be prioritized.

The following will be required in all access control :
a) That all access is prohibited, unless expressly granted.
b) That the entity is uniquely identified [op.acc.1].
c) That the use of resources is protected [op.acc.2].
d) That the following parameters are defined for each entity: what access is required, with what rights and under what authorization [op.acc.4].
e) The persons who authorize, use and control the use will be different [op.acc.3].
f) That the identity of the entity is sufficiently authenticated [op.acc.5].
g) That both local access ([op.acc.6]) and remote access ([op.acc.7]) are controlled.

By complying with all the measures indicated, it will be guaranteed that no one will access resources without authorization. In addition, the use of the system will be recorded ([op.exp.8]) to be able to detect and react to any accidental or deliberate failure.

When systems are interconnected in which identification, authentication and authorization take place in different security domains, under different responsibilities, in cases where it is

necessary, the local security measures will be accompanied by the corresponding collaboration agreements that define mechanisms and procedures for the effective attribution and exercise of the responsibilities of each system ([op.ext]).”

3. And finally, section 4.3.2 relating to "Security Configuration", which determines the following:

"The equipment will be configured prior to its entry into operation, so that:
a) Standard accounts and passwords are withdrawn.
b) The “minimum functionality” rule will apply: (…)”

So, in the case at hand, it has been proven that the data processor, Indra, did not apply basic level technical measures, required by SocMobilitat to guarantee a level of security appropriate to the risk (tending to prevent these data from being unauthorized persons could access), given that when configuring the access control to the T-Mobilitat web portal, the password assigned by default by the manufacturer of the "Liferay" technology infrastructure to the administrator was not modified, in such a way that the access was open, and in turn, accessible to third parties.

This fact recorded in the section on proven facts constitutes the violation provided for in article 83.4.a) of the RGPD, 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 32.1 of the RGPD.

Having said that, the conduct addressed here has been included as a serious infraction in article 73.f) of the LOPDGDD, in the following form:

"f) The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679."

4 . In the data processor contract signed between SocMobilitat and Indra, as has also been said, it was stipulated that Indra had to adopt the basic level measures of the ENS to guarantee a level of security appropriate to the risk, and thus the following was stated:

"7. Obligations of the data controller (...)
"7.5. Safety of Treatment
*The person in charge of the treatment will implement the appropriate measures 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 the confidentiality, integrity, availability and permanent resilience of the Treatment systems and services.
b. Quickly restore availability and access to Personal Data in the event of a physical or technical incident.
c. Verify, evaluate and assess regularly, the effectiveness of the technical and organizational measures implemented to guarantee the safety of the treatment.
d. Pseudonymize and encrypt personal data, if applicable.
Together, it must adopt all those other measures that, taking into account the set of treatments it carries out, are necessary to guarantee a level of security adequate to the risk.

The documentation related to risk management, including the results of the periodic audits that are carried out, can only be requested at any time by the person responsible for the treatment.

In this regard, the tenth section of article 28 of the GDPR provides the following:

" 10. Without prejudice to the provisions of articles 82, 83 and 84, if a person in charge of the treatment infringes these Regulations when determining the purposes and means of the treatment, he must be considered responsible for the treatment with regard to said treatment .”

This is also applicable to the sub-processor, in accordance with the provisions of article 28.4 of the RGPD and 70.1.b) LOPDGDD (which is considered, in any case, a supervisor of the processor), and , therefore, is also responsible, before the control authority, for the alleged violations of the data protection regulations that he may commit in the development of the assignment (technical services entrusted), and specifically for the lack of application of the basic level measures required in the same order, in the configuration of the T-Mobility access portal, without requiring, as has been said, the adoption of any corrective measures, since Indra has accredited having taken the appropriate measures to solve the security incident detected on the platform.

5. When the entity Indra Sistemas SA does not comply with any 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, 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, it is appropriate to impose the penalty of 23,500 euros (twenty-three thousand five -hundreds of euros). This quantification of the fine, in an amount reduced compared to that proposed by the instructor of the procedure, after considering that one of the aggravating circumstances contemplated in the resolution proposal does not apply, is based on the weighting of the aggravating and mitigating criteria that below are indicated:

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

- The nature, gravity and duration of the infringement (art.83.2.a).

- To have taken immediate measures to correct the effects of the infringement.

- The lack of intentionality (art.83.2.b) RGPD).

- The lack of proof of obtaining benefits as a result of the infringement (art. 83. 2. k) RGPD and 76.2. c) LOPDGDD).

Other mitigating criteria invoked by Indra in its fifth allegation do not apply, specifically the mitigating factor provided for in article 83.2.g) of the RGPD, and the one provided for in art.76.2.d) of the LOPDGDD, while, with regard to the first, the nature of the affected data has already been taken into account when applying the mitigation provided for in art.83.2.a) of the RGPD, and that, as regards the second, the action of a third party has had no impact on the commission of the offense charged here, as has already been said repeatedly.

On the other hand, as an aggravating criterion, the following element must be taken into account :

– The linking of Indra's activity with the processing of personal data, having as its main activity the provision of consulting services in different areas, which involves the processing of personal data in the operations and projects it executes for its customers (as stated on the website https://www.indracompany.com/es/indra/privacidad-proteccion-datos).

Nevertheless, the aggravating criterion contemplated in the proposal for resolution referring to article 83.2.e) of the RGPD does not apply, as it has been proven that the previously sanctioned entity was Indra BMB Servicios Digitales SL , which has legal personality independent of the entity imputed here, which must lead to the reduction of the amount of the sanction proposed by the investigating person.

For all this, I resolve:

1 . To impose on Indra Sistemas, SA the penalty consisting of a fine of 23,500.- euros (twenty-three thousand five hundred euros), as responsible for an infringement provided for in article 83.4.a) in relation to the Article 32.1, both of the RGPD, without the need to require corrective measures in accordance with what has been set out in the fourth legal basis.

2 . Notify this resolution to Indra Sistemas, SA.

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 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.