File No: EXP202204816
IMI Reference: A56ID 406200 Case Register 434041

FINAL DECISION

From the actions carried out by the Spanish Data Protection Agency and on the basis of the following

BACKGROUND

FIRST: On 24 December 2021, the Spanish Data Protection Agency received a notification of a personal data breach sent by **INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.** with VAT B62187323 (hereinafter, **INSTITUTO MARQUÉS**), informing that:

Cyber-attack availability breach with potential consequences for those affected. There are indications that data extracted by the breach has been used for sending emails to those affected.

Date of detection of the breach: 21 December 2021.

They state that they communicated the breach to those affected on 29 March 2022 as a result of the knowledge, on 25 March 2022, that the confidentiality of the data had been affected. They became aware of this because INSTITUTO MARQUÉS received an email from the [redacted] account containing its own data extracted from the reporting entity's information systems.

There are data subjects affected in other countries: France, Ireland, Italy, Romania and the United Kingdom.

Number of persons affected according to notification: 400 users, patients and employees.

Data typology according to notification: Identity, image, contact details, financial and means of payment data, health and genetic data.

SECOND: Via the 'Internal Market Information System' ('the IMI System'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), which aims to promote cross-border administrative cooperation, mutual assistance between the Member States and the exchange of information, on 6 June 2022, the Spanish Data Protection Agency (AEPD) declared itself the lead authority in this case. This in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter GDPR), taking into account its cross-border nature and the fact that this Agency is competent to act as lead supervisory authority, given that INSTITUTO MARQUES has its registered office and establishment in Spain.

The processing of data carried out concerns data subjects in several Member States. According to the information incorporated into the IMI System, in accordance with Article 60 of the GDPR, the supervisory authority of Italy acts as a 'concerned supervisory authority' under Article 4 (22) GDPR, since data subjects residing in that Member State are substantially affected or are likely to be substantially affected by the processing which is the subject of these proceedings.

THIRD: On April 18, 2022, the General Subdirectorate for Data Inspection (SGID) received the notification of the personal data breach and opened preliminary investigations to clarify the facts in question, in accordance with the powers of investigation conferred on the supervisory authorities in Article 57 (1) and the powers conferred on them in Article 58 (1) of the GDPR, and in accordance with Title VII, Chapter I, Section II of Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter 'GDPR'), and in accordance with Title VII, Chapter I, Section II of the LOPDGDD, (hereinafter LOPDGDD), having knowledge of the following:

With regard to the undertaking

INSTITUTO MARQUES is a limited company of Spanish nationality. According to the data available in AXESOR, this is a group matrix with 115 employees and a sales volume of [redacted] EUR. No previous procedures relating to this entity's infringements were found in the information systems of this Agency.

Information and documentation have been requested from INSTITUTO MARQUES, and the response received on 27 June 2022, together with the information provided in the notifications of the breach made on 24 December 2021, 15 February 2022 and 30 March 2022, shows the following:

With regard to the chronology of the facts. Actions taken to minimise adverse effects and measures taken for final resolution:

[redacted]

[redacted]

[redacted]

[redacted]

agencia española protección datos

[redacted]

(...)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

On the causes that made the breach possible

[redacted]

With regard to the data concerned

[redacted]

Regarding the processor contract

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

With regard to the security measures put in place

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

FOURTH: On 21 March 2023, the Director of the AEPD adopted a draft decision to initiate penalty proceedings. Following the process set out in Article 60 GDPR, this draft decision was transmitted via IMI on 31 March 2023 and the authorities concerned were informed that they had four weeks from that time to raise relevant and reasoned objections.

The period for processing the present penalty proceedings was automatically suspended during these four weeks, in accordance with the provisions of Article 64(4) of the LOPDGDD.

Within the deadline for that purpose, the supervisory authorities concerned did not raise any relevant and reasoned objections to it, and therefore all the authorities are deemed agree with and are bound by that draft decision, in accordance with Article 60(6) of the GDPR.

This draft decision was notified to INSTITUTO MARQUÉS on 22 March 2023, in accordance with the Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt in the file.

FIFTH: On 13 June 2023, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against INSTITUTO MARQUÉS in order to impose a fine of 80,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP, for the alleged infringements of Articles 5.1.f), 32 and 34 21 of the GDPR, as defined in Article 83 of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was collected by INSTITUTO MARQUÉS on 14 June

2023, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

SIXTH: On 18 October 2023 INSTITUTO MARQUÉS paid the penalty.

The payment made entails the waiver of any action or appeal against the final decision, in relation to the facts referred to in the agreement to initiate penalty proceedings.

LEGAL GROUNDS

I
Competence and applicable law

In accordance with Articles 58.2 and 60 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), and as set out in Articles 47, 48.1, 64.2, 68.1 and 68.2 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD), is competent to adopt this draft decision the Director of the Spanish Data Protection Agency.

In addition, Article 63 (2) of the LOPDGDD states that: '*The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures.*'

II
Preliminary remarks

In the present case, in accordance with Article 4 (1) and (4.2) of the GDPR, there is a processing of personal data, since INSTITUTO MARQUES collects and stores, inter alia, the following personal data of natural persons: identity, image, contact details, economic and payment data, health and genetic data, inter alia processing operations.

INSTITUTO MARQUES carries out this activity in its capacity as controller, as it determines the purposes and means of such an activity, pursuant to Article 4 (7) of the GDPR In addition, this processing is cross-border, as INSTITUTO MARQUÉS is established in Spain, although it serves other countries of the European Union.

The GDPR provides, in Article 56 (1), for cases of cross-border processing, as provided for in Article 4 (23), in relation to the competence of the lead supervisory authority, that, without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for cross-border processing carried out by that controller or processor in accordance with the procedure set out in Article 60. In the case examined, as explained above, INSTITUTO MARQUES is established in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

For its part, Article 4 (12) GDPR broadly defines *'personal data breaches'* (hereinafter the 'security breach') as 'a *breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*.'

In the present case, there is a personal data security breach in the above circumstances, categorised as a breach in confidentiality and availability, as the personal data of at least 400 users have been improperly accessed and the personal data of those users has become inaccessible since 21 December 2021.

Within the principles of processing set out in Article 5 GDPR, the integrity and confidentiality of personal data is guaranteed in Article 5 (1) (f) GDPR. Personal data security is regulated in Articles 32 to 34 of the GDPR, which regulate the security of processing, the notification of a personal data breach to the supervisory authority, and the communication to the data subject, respectively.

III
Principles relating to processing

Article 5 (1) (f) 'Principles relating to processing' of the GDPR provides:

'*1. Personal data shall be*:
(...)

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

In the present case, it is common ground that the personal data of more than 400 users, in the database of INSTITUTO MARQUÉS, were accessed by a third party as a result of the breach of security suffered.

In accordance with the evidence available at this stage, it is considered that the known facts constitute an infringement, attributable to INSTITUTO MARQUÉS, of Article 5.1.f) of the GDPR.

IV
Classification of the infringement of Article 5(1)(f) of the GDPR

The known facts constitute an infringement, attributable to INSTITUTO MARQUÉS as defined in Article 83 (5) of the GDPR, which, under the heading *'General conditions for the imposition of administrative fines'*, provides:

'*Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*

a) the basic *principles for processing, including the conditions for consent under Articles 5, 6, 7 and 9;* (...)'

In this regard, Article 71 of the Spanish LOPDGDD, entitled *'Infringements'*, provides that:

'*The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements*.'

For the purposes of the limitation period, Article 72 *'Very serious infringements'* of the Spanish LOPDGDD states:

'*1. In accordance with article 83.5 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered very serious infringements and its limitation period shall be three years:*

(a) the processing of personal data which infringes the principles and guarantees provided for in article 5 of Regulation (EU) 2016/679. (...)'

V
Sanction for infringement of Article 5(1)(f) GDPR

This infringement may be fined up to 20.000.000 EUR or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 (5) of the GDPR.

In order to decide on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered appropriate to graduate the sanction imposed in accordance with the following criteria established in Article 83.2 of the RGPD:

As aggravating factors:

— The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operation concerned, as well as the number of data subjects concerned and the level of the damages they have suffered (paragraph (a): for undue access to specially protected health data of at least 400 affected persons, from 21 December 2021 to 25 March 2022 at least.

— The categories of personal data concerned by the infringement (paragraph g): In the present case, according to INSTITUTO MARQUES's notification, data of racial origin, health, genetics, among other personal data of those affected would have been disclosed.

As mitigating factors:

— Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly,

through the infringement (paragraph (k): a number of measures were taken, such as [redacted], among others.

The sanction imposed is also graduated in accordance with the following criteria laid down in Article 76(2) '*Penalties and corrective measures'* of the LOPDGDD:

— The link between the offender's activity and the processing of personal data (paragraph b): this is an entity used to the processing of personal health data.

As mitigating factors:

— To have, where this is not compulsory, a data protection officer (paragraph g).

The balance of the circumstances referred to in Article 83.2 of the GDPR and Article 76.2 of the LOPDGDD, with respect to the infringement committed by violating the provisions of Article 5.1.f) of the GDPR, makes it possible to impose a penalty of 50,000 € (fifty thousand euros).

VI
Security of processing

Article 32 "*Security of processing*" of the GDPR provides:

'1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.'

In the present case, at the time of the breach, there are reasonable and sufficient indications that the security measures, both technical and organisational, that INSTITUTO MARQUÉS had in relation to the data it processed, were not adequate.

The consequence of this lack of adequate safety measures was the exposure of 400 users to the health data, race, among other exposed data, to third parties. In other words, those affected have been deprived of control over their personal data.

In the case of particularly protected data, the infringement of which would result in a greater risk to the rights and freedoms of individuals, there is an additional risk that needs to be assessed and that the level of protection with regard to the security and the protection of the integrity and confidentiality of such data is increased.

This risk should be taken into account by the controller who, depending on the controller, should put in place the necessary technical and organisational measures to prevent the loss of control of the data by the controller and thus by the data subjects who provided the data.

The facts described above do not show that INSTITUTO MARQUÉS, as the controller now analysed, has had the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, at least as regards the [redacted] the company.

Therefore, in accordance with the evidence available at this stage, it is considered that the known facts constitute an infringement, attributable to INSTITUTO MARQUÉS, of Article 32 of the GDPR.

VII
Classification of the infringement of Article 32 of the GDPR

The known facts constitute an infringement, attributable to INSTITUTO MARQUÉS as defined in Article 83(4) of the GDPR, which, under the heading '*General conditions for the imposition of* administrative fines*',* provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (...)"

In this regard, Article 71*'Infringements'* of the Spanish LOPDGDD states that '*The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements*'.

For the purposes of the limitation period, Article 73*'Serious infringements*' of the Spanish LOPDGDD states:

'In accordance with article 83.4 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered serious infringements and its limitation period shall be two years:

(...)

(f) Failure to adopt appropriate technical and organizational measures for ensuring a security level appropriate to the risk related to the processing, in the terms required by article 32.1 of Regulation (EU) 2016/679.' (...)

VIII
Sanction for infringement of Article 32 GDPR

This infringement may be fined up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 (5) of the GDPR:

In order to decide on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered appropriate to graduate the sanction imposed in accordance with the following criteria established in Article 83.2 of the RGPD:

As aggravating factors:

— The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operation concerned as well as the number of data subjects concerned and the level of damage suffered by them (paragraph a): the lack of adequate security measures, which made it possible for the data of at least 400 data subjects to be affected by a breach such as that in the present case, which made it possible to infringe the confidentiality of those health data from 21 December 2021 to 25 March 2022 and to make some of those data unavailable from 21 December 2021 to the present day.

— The categories of personal data concerned by the infringement (paragraph g): In the present case, according to the entity's notification, data of racial origin, health, genetic data, among other personal data of the data subjects, would have been compromised.

As mitigating factors:

— Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, through the infringement (paragraph k): the company had a number of (but insufficient) measures in place to prevent a security breach from occurring and subsequently also took measures to improve its security systems, such as [redacted], among others.

The sanction imposed is graduated in accordance with the following criteria laid down in Article 76(2) '*Penalties and corrective measures'* of the Spanish LOPDGDD:

— The existence of a link between the perpetrator's activities and their processing of personal data (paragraph b): this is an entity used to the processing of personal health data.

As mitigating factors:

— The existence of a Data Protection Officer, in those cases when their appointment is not compulsory (paragraph g)

The balance of the circumstances referred to in Article 83.2 of the GDPR and Article 76.2 of the LOPDGDD, with respect to the infringement committed by violating the provisions of Article 32 of the GDPR, makes it possible to impose a penalty of € 20,000 (twenty thousand euros).

IX

Communication of a personal data breach to the data subject

Article 34 *'communication of a personal data breach to the data subject'* of the GDPR provides:

'1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met."

In the present case, the breach entailed a high risk to the rights and freedoms of natural persons. According to the statements made by INSTITUTO MARQUÉS, [redacted]

With regard to the communication to the data subjects, Article 34 (1) of the GDPR states that such communication must be communicated to the data subject without undue delay. In this regard, it does not appear from this file that the communication was made to all *those concerned* who saw their personal data exposed, since the statements of INSTITUTO MARQUES refer to the fact that *'the General Subdirector of INSTITUT MARQUES sent emails to all the actual patient email accounts copied in those communications to inform them of the events*...'. It is clear from this statement that the communication would not have been sent to all persons who could have seen their personal data exposed.

Likewise, the communication would not have taken place 'without the undue delay' laid down in Article 34, in so far as the attack was known on 21 December 2021, and any communications did not start to be made until 25 March 2022, that is to say, three months after the computer attack was recorded, without justifying the reason for that delay.

On the other hand, Article 34 (2) of the GDPR refers to Article 33 of the GDPR in relation to the content of that communication. Thus, the content is that set out in Article 33 (3) (b), (c) and (d) GDPR, which provides:

'3. *The notification referred to in paragraph 1 shall at least:*

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.'

In the present case, the content of the emails sent by INSTITUTO MARQUÉS does not comply with Article 33 of the GDPR in so far as they provided a copy of three of those emails in which it can be seen that they [redacted], but it does not contain the requirements laid down in Article 33 (3) (b), (c) and (d) and 34.2 of the GDPR.

In the present case, the breach entailed a high risk to the rights and freedoms of natural persons, and none of the circumstances listed in Article 34(3) GDPR exempted INSTITUTO MARQUÉS from the duty to inform data subjects that this breach had occurred.

Therefore, in accordance with the evidence available this stage, it is considered that the known facts constitute an infringement, attributable to INSTITUTO MARQUÉS, for violation of Article 34 of the RGPD.

X

Classification of the infringement of Article 34 of the GDPR

The known facts constitute an infringement, attributable to INSTITUTO MARQUES as defined in Article 83(4) of the GDPR, which, under the heading *'*General conditions for the imposition of administrative fines*',* provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

> *(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (...)'*

In this regard, Article 71*'Infringements'* of the Spanish LOPDGDD states *that 'The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements*'.

For the purposes of the limitation period, Article 74 *'Minor infringements*' of the Spanish LOPDGDD states:

'In accordance with sections 4 and 5 of article 83 of Regulation (EU) 2016/679, any infringement consisting on merely formal lack of compliance with the provisions mentioned therein, especially the ones listed below, shall be considered a minor infringement and its limitation period shall be one year:

> *"(...)*

ñ) Failure to comply with the duty of reporting to the data subject any data security breach which is considered highly hazardous for the rights and liberties of data subjects, pursuant to the requirements of article 34 of Regulation (EU) 2016/679, unless the provisions set forth in article 73 s) of this organic law apply. (...)"

XI
Sanction for infringement of Article 34 GDPR

This infringement may be fined up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 (5) of the GDPR:

In order to decide on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered appropriate to graduate the sanction imposed in accordance with the following criteria established in Article 83.2 of the RGPD:

As aggravating factors:

— The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operation concerned as well as the number of data subjects concerned and the level of damage suffered by them (paragraph a): By failing to inform the data subjects, at least 400, that the security breach in question had occurred, and by failing to communicate all the information required by Article 34 (2) GDPR without undue delay (between 21 December 2021 and 25 March 2022) to those affected by that communication.

— The categories of personal data affected by the infringement (paragraph g): In the present case, according to the INSTITUTO MARQUES's notification, data of racial origin, health, genetic data, among other personal data of the data subjects, would have been compromised.

As mitigating factors:

— Any measure taken by the controller or processor to mitigate the damage suffered by data subjects (paragraph c): partial or incomplete information on the existence of the breach was provided to some affected.

We also consider that the sanction to be imposed should be graduated in accordance with the following criteria laid down in Article 76(2) '*Penalties and corrective measures'* of the LOPDGDD:

— The existence of a link between the perpetrator's activities and their processing of personal data (paragraph b): this is an entity used for the processing of personal health data.

As mitigating factors:

— The existence of a Data Protection Officer, in those cases when their appointment is not compulsory (paragraph g).

The balance of the circumstances referred to in Article 83.2 of the GDPR and Article 76.2 of the LOPDGDD, with respect to the infringement committed by violating the provisions of Article 34 of the GDPR, makes it possible to impose a penalty of 10.000 EUR (ten thousand euros).

XII
Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled *'Termination in penalty* proceedings', provides:

'*1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.*

2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (…)'

According to the above,
the Director of the Spanish Agency for Data Protection DECIDES TO:

FIRST: DECLARE the termination of proceeding **EXP202204816** in accordance with Article 85 of the LPACAP.

SECOND: NOTIFY this resolution to **INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.**.

In accordance with the provisions of Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the fourth additional provision of Law 29/1998 of 13 July governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

936-040822

Mar España Martí
Director of the Spanish Data Protection Agency