apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 50/2020, referring to the Terrassa Mutual Assistance Foundation

Background

1. On 07/08/2019, the Catalan Data Protection Authority received a letter from a person filing a complaint against the Fundació Assistencial Mútua de Terrassa (hereinafter, FAMT) on the grounds of a alleged breach of the regulations on personal data protection.

Specifically, the complainant ((...)) stated the following:

- That on (...)/2019 he had scheduled a surgical intervention at ÀPTIMA Center Clínic (belonging to the Terrassa Mutual Group), the center he had attended to receive private medical assistance.
- That on the same day a nurse informed him that they were canceling his intervention based on certain information that was contained in his medical history available at the Primary Care Center (...)-managed by the FAMT of Grup Mútua de Terrassa, of which the complainant here is a user.
- That on (...)2019, in a telephone conversation with her doctor from ÀPTIMA, she complained about her access to her CAP medical history *"when she herself had told me on several occasions that she was separated from which was the mutual of Terrassa (public health) of Àptima, as they are a private clinic".* Faced with this, the doctor replied that *"they had permission to access".*
- That *"at no time did I sign a consent document to access my clinical data and that curiously on July 23, 2019 when I went to my CAP in (...) (which belongs to the Terrassa Mutual), to make some arrangements at the service desk, they gave me a document to sign, not being able to read it, three days later I went to ask for a copy to know that I had signed because I was left with doubt and curiously it was a consent to access my data from the Terrassa Mutual Assistance Foundation where it also names Aptima Clínic Centre".*

The complainant, in relation to the facts exposed, complained, on the one hand, to the FAMT *"for allowing a private entity (Àptima Center Clínic) access* to his medical records from the CAP (...); and, on the other hand, to Dra. (...) of ÀPTIMA, for having made *"improper use"* of certain medical information contained in said history.

The complainant provided, among other information, a copy of a document printed on 26/07/2019, with the logo of the Mútua de Terrassa, entitled *"Informed consent.*
Consent for use of personal data", which contains the following text:

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

"In accordance with the provisions of Regulation (EU) 2018/679 of the European Parliament and of the Council (...), we inform you that your personal data, both administrative and health, are subject to professional secrecy. FUNDACIÓ ASISTENCIAL DE MÚTUA DE TERRASSA FPC, with NIF (...), FUNDACIÓ VALLPARADÍS, FPC, with NIF (...), and ÀPTIMA CENTER CLÍNIC, SL, with NIF (...), are responsible for the treatment of the data, and have appointed a Data Protection Delegate, who can be contacted by email (...).

The purpose of the data processing will be to ensure the registration and monitoring of the medical treatment provided, to ensure the continuum of care between the different health and social devices; provide the necessary information for the correct invoicing of the cost of the services provided, complete your clinical history (HC) in the center and implement the mechanisms for coordinating clinical histories that are developed. This information will be used by the administrative services and services directly linked to the health care of our entity, each in their own competences, and may be sent in whole or in part to official public or private entities that, for legal reasons or material need, must access the data for the purpose of the correct provision of medical assistance. (...)"

2. The Authority opened a preliminary information phase (no. IP 226/2019), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts they were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

3. In this information phase, by means of a letter dated 10/14/2019, the reported entity was required to comply with the following:

- Provide a copy of the record of access to the medical history of the person making the complaint from the CAP of (...), in the period between 04/11/2019 and (...)/ 2019, both included.

- Indicate the reasons that would justify each of the accesses made in this period.

4. On 10/28/2019, the reported entity responded to the aforementioned request in writing in which it stated the following:

a) That between 11/04/2019 and (...)/2019 a total of 8 accesses to the medical history of the complainant were recorded, of which 3 correspond to the Hospital Universitari Mútua de Terrassa (FAMT) , 2 in CAP (...) (FAMT), and 3 in ÀPTIMA.
The log of accesses to the medical history of the reporting person between 04/11/2019 and (...)/2019 is provided as DOC1.
b) That *"all users who have accessed the patient's clinical history are properly identified, and all consultations carried out both by FAMT and by ÀPTIMA respond to the purpose of processing medical assistance -sanitary of this*

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

patient, who was treated by both FAMT and ÀPTIMA". The access details are as follows:

- 11/04/2019 access from Hospital Universitari Mútua Terrassa (FAMT) by "Person 1", FAMT employee, with an administrative profile. Consulted data: administrative (intervention programming).
- 04/14/2019 access from CAP (...) (FAMT), by "Person 2", FAMT employee, with administrative profile. Data consulted: administrative (appointment scheduling).
- 04/14/2019 access from CAP (...) (FAMT), by "Person 3", FAMT worker with medical profile Data consulted: health data.
- (...)/2019 access from Hospital Universitari Mútua Terrassa (FAMT) by "Person 4", FAMT employee, with an administrative profile. Data consulted: administrative (admissions).

- (...)/2019 access from ÀPTIMA, by "Persona 5", employee of *"TRACTAMENT ESTETIC TERRASSA, SL that provides services to ÀPTIMA",* with an administrative profile. Data consulted: administrative (appointment scheduling).
- (...)/2019 access from Hospital Universitari Mútua Terrassa (FAMT) by "Persona 6", FAMT employee, with an administrative profile. Data consulted: administrative (appointment scheduling). • (...)/2019 access from ÀPTIMA, by Dra. (...) (doctor identified by the complainant)", employee of *"TRACTAMENT ESTETIC TERRASSA, SL that provides services to ÀPTIMA",* with a medical profile. Data consulted: health data.

- (...)/2019 access from ÀPTIMA, by "Persona 8", employee of ÀPTIMA, with profile administrative Data consulted: administrative (appointment scheduling).

c) That, with regard to the complainant's complaint regarding improper access by an ÀPTIMA medical professional to the medical history available to the CAP (...), it should be noted that this person signed on the dates 09/05/2016 and 07/23/2019 - on the occasion of the entry into force of the European Regulation on the protection of personal data - two documents through which *"this patient was provided with the mandatory information about the processing of personal data by FAMT and APTIMA, in accordance with what is provided for in articles 5-7 of the old LOPD 15/99 and in article 13 of the RGPD".*
The referred documents signed by the reporting person are provided as DOC2 and DOC3.

d) That FAMT and ÀPTIMA are *"joint owners"* of the "Patient" file, as was informed at the time to the Spanish Data Protection Agency (hereafter, AEPD), when it was registered .

The communications to the AEPD, *"about the co-ownership of this patient file" ,* are provided as DOC4 and DOC5 .

e) That *"in addition to their capacity as responsible for the same patient file, FAMT and ÀPTIMA also maintain a contractual relationship for the provision of health services by FAMT to ÀPTIMA, which requires access by FAMT, in quality of the person in charge of the treatment, in the patient file of which both parties are joint owners".*
Attached as DOC6 is *the "services and data processing contract, which was updated on 05/25/2018"*

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

f) That *"the private medical services offered by ÀPTIMA to its users are provided by self-employed professionals or companies, which maintain a commercial relationship with ÀPTIMA".*
Attached as DOC7 is *"the contract for services and the processing of personal data signed between TRACTAMENT ESTÈTIC TERRASSA, SL and ÀPTIMA on (...)2018"*

g) That *"all FAMT and ÀPTIMA workers and collaborators with access to the patient database undertake in writing to respect confidentiality, professional secrecy and the regulations on personal data protection".*

h) That *"we consider that access to the claimant's HC by ÀPTIMA is legitimate when to what":*

- *"ÀPTIMA is joint owner of the patient file of FAMT and the Vallparadís FPC Foundation, as reported to the AEPD. It has been certified that the claimant has received and signed as a sign of knowledge and consent the letter informing about the circumstances of the processing of her personal data. Therefore, there is no transfer of data because at the time of data collection, the interested party was informed that both ÀPTIMA and FAMT are responsible for the treatment of the clinical history database".*
- *"ÀPTIMA and FAMT also maintain a service provision relationship, in which ÀPTIMA is responsible and FAMT is in charge. In this context, access was carried out from the FAMT University Hospital by the centre's administrative staff".*

- Dr. (...) *"is a medical professional who provides her services to ÀPTIMA, with whom the company (...) (TRACTAMENT ESTETIC TERRASSA SL) signed the corresponding service contract containing the clauses that regulate the conditions of the treatment of ÀPTIMA patient data, in its capacity as the person in charge of the treatment.*
  The administrator (PERSON 5) is an employee of the professional society in charge of the treatment".

The reported entity, as has been advanced, attached various documentation to the letter:

- DOC1 (cited in section a). Record of accesses to the medical history of the reporting person during the period between 04/11/2019 and (...)/2019.
- DOC2 and DOC3 (cited in section c). *"Consent to use of personal data"* documents
  - DOC2. This document, which does not contain any date, contains the handwritten signature of the person making the complaint. According to the FAMT in its letter, this document would have been signed by the complainant on 09/05/2016.
    This document contains the following text:
    "In accordance with the provisions of Law 15/1999 on Data Protection and its development regulations, we inform you that your personal data, both administrative and health, are subject to professional secrecy and will become part of a PATIENT FILE co-owned by the MÚTUA DE TERRASSA MUTUALITY SOCIAL PENSION A PRIMA FIXA entities; OPTIMA CLINICAL CENTER; I FUNDACIÓ VALLPARADÍS-CATALAN PRIVATE FOUNDATION.

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

The purpose of the treatment of this data is the provision of the medical health service to patients, and, in particular, the formalization of their clinical history and the performance of administration and invoicing tasks that correspond.
The recipients of the data are the people and departments responsible for the assistance provided, as well as the entities of the Mútua Terrassa Group called CATLAB AND DIAGNOSTIC TECHNOLOGY CENTER that, due to material needs or legal imperative, must access their data for to the correct provision of medical-sanitary assistance".

• DOC3. This document has the same content as the one provided by the person making the complaint (1st record), with the difference that it contains the handwritten signature of the person making the complaint, and was printed on 07/23/2019.

- DOC4 and DOC5 (cited in section d) registration and modification notifications, respectively, of the "Pacientes" file in the AEPD. In the document *"Informe de situación de inscripción en Registro de protección de datos"* issued by the AEPD on 09/18/2017, the following is indicated in relation to the "Pacientes" file:

"Responsible and Management: Fundació Assistencial de Mútua de Terrassa, FPC (...)
Description of the purpose; patient file under co-ownership regime for the entities of Grupo Mútua de Terrassa, (Mútua de Terrassa, Mutualidad de Previsió Social a Prima Fixa, Àptima Center Clínic SL, Fundació Vallparadís, Fundació Privada Catalana), in the treatment of data that is necessary for the provision of health and social assistance".

- DOC6 (cited in section e). *"Contract for the provision of Services"* formalized on 05/25/2018 between ÀPTIMA and FAMT, which contains the following text: *"Object FAMT undertakes to provide ÀPTIMA - with all the personal and technical means it has in its facilities located in the HUMT building - the hospital health services you require and which are detailed below, for the assistance of the people treated by ÀPTIMA: emergency room, operating rooms, delivery room, anesthesiology and resuscitation , Radiology and CAT (...)*

Financial conditions:
ÀPTIMA will pay FAMT for each of the individual services it provides to its customers, whether or not admitted to its premises, according to the price tariff (...)
Duration: This contract is agreed for a duration of three years, extendable from year to year (...)

Protection of personal information:
For the provision of contracted services, it is necessary for FAMT to have access to and carry out the processing of personal data of patients on behalf of ÀPTIMA, so both parties are obliged to comply with Regulation (EU) 2016/679 (...) .
For the execution of the agreed services, FAMT will treat on behalf of ÀPTIMA the information with personal data that is detailed:

ÿ *As categories of interested parties, data from ÀPTIMA users/ patients will be processed* ÿ *As types of data, identification and health data will be* processed

the interesting ones

ÿ *Particularly sensitive data. Health data*

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

The aforementioned information is collected in the patient file of which both parties are joint owners, in accordance with the agreement signed between the parties on January 1, 2014, in order to work with a comprehensive system in the matter of data protection that allows improving care circuits and optimizing the systems and resources they have.
FAMT will use the personal data that is the subject of treatment, or that it collects for its inclusion, only for the purpose of this assignment. Under no circumstances may you use the data for your own purposes. Also, it will not communicate the data to third parties, unless it has the express authorization of APTIMA and in admissible cases.
FAMT will not be able to subcontract (...) except for the necessary auxiliary services (...). The subcontractor, who will also have the status of processor, is also obliged to comply with the obligations established in this document for the processor and the instructions issued by ÀPTIMA.

- DOC7 (cited in section f). Service contract formalized on (...)2018 between APTIMA and Tracamento Estétic Terrassa SL ((...). (...), in which the following text is included:
"They state:

I. That ÀPTIMA has facilities located in several localities (...) in which they offer outpatient services for medical consultations, surgery, diagnostic imaging and in vitro fertilization.

II. That ÀPTIMA (...) has signed a collaboration contract with Fundació Assistencial Mútua de Terrassa, whereby the Mútua Terrassa University Hospital (henceforth, HUMT) makes available to ÀPTIMA all the personal and technical services of has for the health care of patients.

III. That the health services offered by ÀPTIMA are aimed at private patients (direct payment) and patients from health insurance companies with whom ÀPTIMA has signed collaboration agreements.

IV. That the Tractament Estétic Terrassa society has a special interest in exercising its profession through private medicine and wishes to do so at the ÀPTIMA facilities (...)
VI. At the same time, ÀPTIMA has an interest in making this collaboration possible.
(...)
Pacts:

first The object of this contract is the provision of professional medical services by Tractainment Estétic Terrassa in the specialty of (...) to private patients of ÀPTIMA or who come from health insurance companies, such as patients of society itself (sic).

For the provision of these services, ÀPTIMA cedes the use of a space for a medical office to the company Tractament Estètic Terrassa (...)
second On the other hand, ÀPTIMA will make available to the company the material and personal resources described in Annex 1 (Service, economic and professional conditions) so that they can carry out their assistance work, for the provision of services by the company Aesthetic Treatment Terrassa (...).

third For the contracted professional actions that take place in the medical office of ÀPTIMA, the company Tractament Estètic Terrassa undertakes to enter and intervene with private and company patients, solely and exclusively in the facilities assigned by ÀPTIMA which will specifically be the ÀPTIMA and/or HUMT hospitalization clinic (...).

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

(...)
sixth In compliance with the legislation in force regarding the protection of personal data, as well as regarding clinical documentation, the company Tractament Estètic Terrassa assumes the following obligations and responsibilities:
a) In accordance with current legislation on data protection (...) access to the database of ÀPTIMA and/or, as the case may be, of Fundació Assistencial Mútua de Terrassa will be made, only and exclusively, to provide health care to the patients they have to attend, complying with the duty of professional secrecy and confidentiality. (...)
b) Treat the personal data to which you have access in accordance with the instructions of ÀPTIMA, which will be the entity responsible for the file (...) The clinical histories will be guarded by ÀPTIMA.
c) (...)
d) Not to communicate the access keys to the ÀPTIMA database to third parties makes available (...)
(...)
It is guaranteed that, without prejudice to the exact compliance with everything established in this document, the provisions of the current regulations on the matter as well as the internal regulations on confidentiality and use of APTIMA information systems, Annex 3

(...)"

5. In view of the information provided by the FAMT, on 11/11/2019, additional information was requested from the reported entity, including:

- Confirm that in the file (database) of clinical histories co-ownership of the FAMT, Fundació Vallparadís and ÀPTIMA - from now on, the "Pacients" file - includes the clinical histories of the people/patients who are users of public health care who go to the centers managed by the Mútua de Terrassa group.
- Confirm that ÀPTIMA staff, by means of username and password, can logically and without any restrictions access the clinical history file mentioned in the previous section.

- Accredit the date of signature by the person making the complaint, of the document *"Consent to use of personal data" (identified* as DOC2).
- Provide a copy of the Treatment Activity Register (hereafter, RAT) of the Terrassa Mutual Group.

6. On 25/11/2019 the FAMT responded to the previous request, by means of a letter in which it stated the following:

- That, *"in the shared file there are all the cynical histories, which are instrumented by patient, regardless of whether this comes from public health (FAMT and the socio-sanitary area of the Vallparadís Foundation), private (Àptima), or both care areas".*
- That, *"in accordance with what is established in article 11 of Law 21/2000 of September 29, on the rights of information concerning the patient's health and autonomy, not all*

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

Àptima workers and collaborators have access to it, as do not all FAMT or Fundació Vallparadís workers, but only those who require it for the performance of their tasks, who are assigned an access code personal and non-transferable user and a profile of permissions, privileges and access to screens appropriate to the professional level, area and center where they develop their services (...)".

- That, with regard to the accreditation of the date of signature, by the complainant here, of the document *"Consent for the use of personal data" (identified* as DOC2), since no data appears in the aforementioned document , *"the only data that we know for sure is the date on which this document was digitized and linked to his medical record no. 49(...) of the patient database, and the date we know is 09/05/2016 (...). In the file system where the consent documents for the use of data in PDF format are stored, there is also the PDF of clinical history no. 49(...) with that date 05/09/2016)" .* Screenshots are provided that would prove the ends indicated.

Along with his letter, he provided a copy of the RAT *"of the PATIENTS of the Foundation entities Mútua de Terrassa Assistance, FPC and ÀPTIMA Center Clínic SL",* with the following details:

- RAT corresponding to the entity *"Mútua e Terrassa Assistance Foundation, FPC"*
  Denomination of the treatment *"Patients".*
  "Purpose of treatments. Assistance provision and planning of medical visits"
  "Legal basis of the Treatments: Art 9.2 h RGPD"
  "Categories of interested parties: Patients of the centers of Aptima Clinical Center, of the Foundation Mútua de Terrassa FPC and Fundació Vallparadís FPC.
  (...)
  Additional information. Correspondents:, Àptima Center Clínic and Fundació Vallparadís, FPC."
- RAT corresponding to the entity *Àptima Center Clínic SL"*
  Denomination of the treatment *"Patients".*
  "Purpose of treatments. Providing assistance to patients of Àptima Center Clínic, planning medical visits, offering services provided by Àptima"
  "Legal basis of the Treatments: Art 9.2 h (medical assistance) and 6.1 a (offer of other services) of the RGPD"
  "Categories of interested parties: Patients of the centers of Aptima Clinical Center, of the Foundation Mútua de Terrassa FPC and Fundació Vallparadís FPC.
  (...)
  Additional information. Correspondents: Fundació Asistencianal de Mútua e Terrassa, FPC and Fundació Vallparadís, FPC."

7. On 09/12/2019 and still within the framework of this preliminary information phase, the Authority again requested additional information from the FAMT, specifically:

- Provide a copy of the internal document of the Terrassa Mutual Group -valid in April 2019- in which the professional profiles with access to the "Patients" file (database) of clinical histories co-owned by the Mutual Care Foundation of

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

Terrassa, Fundació Vallparadís and ÀPTIMA (henceforth, "FITXER"); as well as the functionalities and actions associated with each profile.

- Indicate if Dra. (...), through his username and password, he was able to access in April 2019, not only the medical history of the person reporting here, but also the medical histories of the people listed in the FILE for having received solely and exclusively public health care by the FAMT. If so, please indicate whether this access was also allowed in April 2019 to all professionals with an access profile like the one associated with Dr. (...).

- Report if the doctors who provide service at the APTIMA branches - either as APTIMA's own staff, or as staff from an external company (such as Dra. (...)) - and to whom Grup Mútua de Terrassa enables access to the FILE using user/password, they could access in April 2019 all the clinical histories included in the FILE, regardless of whether the patient was included in the same for having received public or private healthcare from the Terrassa Mutual Group.
- Report if the situation described in the previous section occurred in April 2019 with the rest of the profiles with access to the FILE (nurses, nursing assistants, administrative staff, etc.).

8. On 12/20/2019, the FAMT responded to the previous request, by means of a letter in which it set out the following:

- That *"Dr. (...) and professionals with their same access profile to the FILE ("Aptima Hospital Doctor" and "Aptima Practice Doctor"), operationally have the possibility to access the clinical histories of all the patients listed in this database regardless of who is the guarantor of the medical services provided (CatSalut, a mutual fund or insurance company contracted by the patient, or if the cost of these is assumed by the patient himself). With respect to the rest of the user profiles (nurses, nursing assistants, administrative staff, etc.), the powers of access to patient data also do not depend on the guarantor who assumes the cost of the assistance, but on the specific needs to carry out their functions within the entity.*

  However, despite the technical possibility of accessing all the patients in the FILE, the information about them that can be accessed will depend on the permissions and privileges corresponding to the profile(s) assigned to each user ".
- That *"Dr. (...) as well as the other professionals who maintain a contractual service relationship with ÀPTIMA in addition to the aforementioned internal regulations document (for use of systems), have signed the corresponding contract for the processing of data where they are collected the specific instructions to be followed by the person in charge who will carry out the processing of patient data on behalf of the person in charge (...)".*
- That *"with regard to employees with an employment contract at Aptima, in addition to internal regulations and training, the entity makes available, through the corporate intranet, a document that contains the guidelines for the use of the clinical histories, in which it is made clear that only medical professionals and administrative staff who are carrying out a care process with the specific patient can access patient data".*

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

- That *"in addition to having been informed of the joint ownership of the patient file to the Spanish Data Protection Agency, the patients and users of our organization's services have also been informed in writing of this end. In this specific case, it has been proven that the complainant had been informed - on two occasions - about the joint ownership of the patient file, and on both occasions she had signed as a sign of conformity, and we do not know that she has exercised at any time , neither before FAMT nor ÀPTIMA, a request for exercise on the processing of your personal data".*

Along with its letter, the FAMT provided, among other documents, part of the document entitled *"Patient Safety Document"* of the Terrassa Mutual Group, version *"V6 November 2018",* which includes the following text:

"1. OBJECT

This Patient Safety Document responds to the obligation established in the Regulation European (EU) 2016/679 (...) as well as art. 88 of Royal Decree 1720/2007 (...).

According to the aforementioned article, the Security Document can be unique and include all files or treatments, or individualized for each file or treatment. Different security documents can also be prepared by grouping files or treatments according to the treatment system used for your organization, or by taking into account the organizational criteria of the person in charge.

In any case, it has the character of an internal document of the organization.

Based on the above, and in accordance with art. 26 of the RGPD, this Patient Safety Document applies to the 3 companies of the Mútua Terrassa Group that carry out healthcare activities, specifically:

FUNDACIÓ ASSISTENCIAL MÚTUA TERRASSA, FPC: is the parent company of the entire Group and the one with the most equipment. It currently includes the service provided at the same Hospital Mútua Terrassa and in the primary care centers. The patients he treats are mostly from the Catalan Health Service, but there are also patients from insurance companies.

ÀPTIMA CENTER CLÍNIC, S: is the company that includes the private clinic service of the Group. Therefore, the patients are always either private or from insurance companies.

FUNDACIÓ VALLPARADÍS-FUNDACIÓ PRIVADA CATALANA, FPC: is the company with the social purpose of providing assistance to dependent people, such as the elderly or people with intellectual disabilities, its activity covering both the public and private sectors. (...)

2. SCOPE OF APPLICATION

The decision to proceed with the preparation of a Patient Safety Document that applies to the three companies mentioned in the previous section does not respond in any case to a one-off decision at Group level, but is simply the translation into the sphere of data protection of what the integration of the Mútua Terrassa Group means in terms of patient data management.

This new reality of single and integrated management, both in terms of care circuits and human resources and systems, naturally entails a close link between the aforementioned entities which, in practice, means that there is continuous access and transmission of

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

personal data among them, in their fields of action at the welfare and socio-health level.

(...)

In this sense, this Security Document aims to explain the rules that the Terrassa Mutual Group follows for its internal management, bearing in mind that there are no objective and general legal rules in this regard, and that the fact of establishing a restrictive application of the rules governing access to clinical history and personal data in general, could cause harm to the patient.

Therefore, it is the responsibility of Grup Mútua Terrassa to develop and document through this Security Document the adequacy to the data protection regulations of this reality (...)

3. PATIENT FILE

(...) the option of tending towards joint ownership of the Patient File is closely linked to the health sector regulations themselves, as well as in relation to projects such as the Història Clínica Compartida de Catalunya (HC3), coinciding with the ideas of the maximum possible integration of the clinical documentation and the help to guarantee the adequate assistance of the patient and for this purpose, the care professionals who are involved.

Having said that, the Mútua Terrassa Group as a whole and, in particular, the entities to which this Patient Safety Document applies, are aware of the requirements set out in the current regulations on the protection of personal data (Regulation European (EU) 2016/679 of the Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data; Organic Law 3/ 2018, of December 5, on Protection of Personal Data and guarantee of digital rights and Royal Decree 1720/2007, of December 21, which approves the Regulation for the development of the former Organic Law 15/1999, of December 13, Protection of Personal Data).

Therefore, a single file is structured through a joint ownership of the 3 entities, giving as a result, as it has already been developed, a better integration of information, accessibility and availability to users than the require at all times to provide correct care.

(...)

5.3.1. GROUP AGREEMENT

As we have already developed in section 2 of this Security Document, with the integrated management system, by definition, continuous accesses and transmissions of personal data occur between each of Mútua Terrassa's companies. In this sense, as they are legally independent entities, contracts/ treatment agreements must be signed between them, according to the corresponding legal regime.

We can distinguish 2 types of agreements within the scope of application of the 3 companies that are within the scope of application of this Security Document: • Agreement on co-ownership of patient data files between Fundació Assistencial Mútua Terrassa , Àptima Center Clínic SA and Fundació Vallparadís FPC

(...)

• Agreement for the protection of personal data in communications and data access between the companies of the Mútua Terrassa Group

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

Signed on July 1, 2016 by all the companies of the Mútua Terrassa Group, it is constituted as the framework agreement that regulates access and transmission of data between all of them, obliging themselves to respect the requirements that the protection regulations of data establishes and generally develops each of the ends provided for in art. 12 of LOPD 15/1999, in force at that time. In these terms the Spanish Data Protection Agency has expressed itself through its Legal Report 0494/2008.

(...)

5.4. OBLIGATIONS OF USERS

All the staff of the 3 companies who have access to the personal data of patients, i. intervenes and carries out data processing, is obliged to comply with the provisions of this document.

(...)

The last awareness-raising measure carried out was the mass sending to all users of a reminder email of the merger, from January 1, 2015, to a single clinical history between the 3 Mútua Terrassa entities (. ..)

Subject: Internal announcement Clinical History

Committee All professionals with access to the electronic Clinical History of Mútua de Terrassa (HCIS) are reminded that since 01/01/2015 the tool incorporates information from both private activities and the public activity The fact of having a shared Clinical History allows to guarantee the continuity of care with a better knowledge of the patients and, therefore, favoring that the decisions taken regarding the diagnosis and treatment are more accurate, thus improving the quality user assistance, without affecting security or the service coverage regime.

It is also reminded of the duty of all professionals to comply with the entity's internal regulations on confidentiality and use of information systems, and subjection to legal and ethical regulations in relation to the treatment of patient data .

(...)

6.1.4.2. LOGICAL ACCESS POLICY

(...)

The clinical history is an instrument primarily intended to help guarantee adequate assistance to the patient. For this purpose, the care professionals of the center who are involved in the diagnosis or treatment of the patient must have access to the clinical history.

Each center must establish the mechanism that makes it possible that, while assistance is provided to a specific patient, the professionals attending to him can, at all times, have access to the corresponding medical history. However, the staff who take care of the administration and management tasks of the health centers can access only the data of the clinical history related to said functions,

(...)

In the case of the Patient File of Mútua Terrassa's healthcare entities, a new unique and integrated management reality has been set up that involves a close link between the aforementioned entities which, in practice, generates access and transmissions of character data staff among them, in their fields of action at the welfare and socio-health level. Remember, in this sense, that everything is always for the benefit of the patient

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

(...)".

9. On 30/10/2021, the director of the Catalan Data Protection Authority agreed to start a disciplinary procedure against the FAMT, for four alleged infringements: a first infringement provided for in article 83.4.a), in relation to article 25.2 relating to data protection by design and by default; a second infringement provided for in article 83.5.a), in relation to articles 5.1.a), 6 and 9 referring to the principle of legality with regard to the processing of special categories of data; a third violation provided for in article 83.5.a), in relation to article 5.1.b) and 6.4 referring to the principle of purpose limitation; and a fourth violation provided for in article 83.5.a), in relation to article 5.1.a) referring to the principle of loyalty; all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 02/11/2020.

10. The initiation agreement explained the reasons why no imputation was made with respect to the fact reported relative to the use of the health data of the person here reporting by Dra. (...). In this sense, it was determined that *"it is not up to this Authority to settle the eventual responsibility committed for a possible violation of data protection regulations, to the extent that this doctor carried out the reported treatment as an employee of the company Tractament Estétic Terrassa SL, and this entity would be outside the jurisdiction of this Authority, in accordance with the provisions of article 3 of Law 32/2010, of October 1. Having said that, it must be emphasized that this use would have been facilitated by the facts that are imputed in this sanctioning procedure and that motivate its initiation".*

11. In the initiation agreement, the accused entity was granted a period of 10 working days, counting from the day after the notification, to formulate allegations and propose the practice of evidence that it considered appropriate to defend their interests.

12. On 11/17/2020, the FAMT submitted objections to the initiation agreement.

13. On 05/03/2021, 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 60,000 euros on the FAMT as responsible for an offense classified in article 83.5.a), in relation to article 5.1.a), with regard to the principle of legality (infringement that subsumes violations of the principles of limitation of purpose and loyalty, given their connection); in ideal competition with the infringement provided for in article 83.4.a) in relation to article 25 regarding data protection by design and by default, all of them of the RGPD.

This resolution proposal was notified on 11/03/2020 and a period of 10 days was granted to formulate allegations.

14. On 03/25/2021, the accused entity submitted a statement of objections to the proposed resolution.

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

proven facts

The Fundació Assistencial Mútua de Terrassa (FAMT) and ÀPTIMA Clínic Center (ÀPTIMA), are part of the Terrassa Mutual Group, dedicated to the provision of health services.

The FAMT provides health services through the Terrassa Mutual Hospital and the primary care centers it manages, which are part of the public health system. As the FAMT has stated, the vast majority of patients treated by this entity are from the Catalan Health Service, that is to say, they are treated on behalf of the public health system.

The ÀPTIMA company provides private healthcare services, through private insurers or through direct payment by the user. To provide this assistance, ÀPTIMA has, among others, both its own staff and staff from external companies that provide their services on behalf of ÀPTIMA, as would be the case with the company Tracamento Estétic Terrassa.

Within the framework of this organization, the following facts are considered proven:

1. All the electronic medical records of the Group's patients make up a single common database for the entire Terrassa Mutual Group (HCE), which incorporates information from both the private and public activities of the Group ; and which can be consulted through the information systems available to each entity.

In turn, the data of each of the patients treated by any of the companies that make up the Terrassa Mutual Group are incorporated into an electronic medical history, which is unique for each patient regardless of the regime - public, private or both - in which he has been served by one of the Group's entities.

In line with the above, the data of FAMT patients who have been treated by professionals of this entity under the public health regime, are included in their electronic medical history, which can be consulted by all professionals who they provide service, both to FAMT and APTIMA, through their information systems (using user and password) with no more restriction than that derived from their professional access profile.

2. The health data of the person reporting here collected by the FAMT and contained in its files, were processed on the dates and by the persons indicated below (all of them unrelated to the FAMT and the public provision of services healthcare), without the explicit consent of the affected person and without the concurrence of any other legal basis that legitimizes these treatments.

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

- (...)/2019 access from ÀPTIMA, by "Persona 5", employee of *"TRACTAMENT ESTETIC TERRASSA, SL that provides services to ÀPTIMA",* with an administrative profile. Data consulted: administrative (appointment scheduling).
- (...)/2019 access from ÀPTIMA, by Dra. (...) (doctor identified by the complainant)", employee of *"TRACTAMENT ESTETIC TERRASSA, SL that provides services to ÀPTIMA",* with a medical profile. Data consulted: health data.
- (...)/2019 access from ÀPTIMA, by "Persona 8", employee of ÀPTIMA, with profile administrative Data consulted: administrative (appointment scheduling).

3. The health data of the reporting person, which had been collected by the FAMT with the purpose of providing medical assistance within the public health system, were processed in (...)/2019 for a different and incompatible purpose , specifically in the context of private medical assistance provided to the complainant by the company ÀPTIMA.

4. On 05/09/2016, the FAMT would have informed the person making the complaint through the document entitled *"Consent for the use of personal data" (4th* record, DOC2), that *"his personal data, both administrative and health, are subject to professional secrecy and will become part of a PATIENT FILE co-owned by the Mútua de Terrassa-Mutualitat de Previsión Social a Prima Fixa entities; Aptima Clinical Center; and Foundation Vallparadís - Catalan Private Foundation";* and, that *"the purpose of the treatment of these data is the provision of the medical health service to patients, and, specifically, the formalization of their clinical history and the performance of administration and invoicing tasks that correspond".*

Based on this information, and also on what any user of the public health system can reasonably expect when they go to a primary care center, it was generated in
the person here denouncing the -erroneous- expectation that the treatment of health data collected by the FAMT as part of the health care provided within the framework of the public health system, would always and at all times be carried out in the framework of this type of provision, when the truth is that all the staff of the Terrassa Mutual Group with access to the Group's clinical history database in electronic format - whether or not they were related to the public health system - could access in your medical history (according to your professional profile).

Fundamentals of law

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

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

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

2.1. About the *"lack of competence of the APDCAT"*

In its statement of objections to the proposed resolution, the FAMT alleges a lack of competence on the part of this Authority to initiate disciplinary proceedings against said entity.

In this regard, it must be said that the FAMT provides public health services in concert with the Catalan Health Service, and in this sense, is part of the comprehensive system of public use of Catalonia SISCAT- (Decree 196/2010), acting as responsible for the processing of the data collected based on the provision of public health services. Therefore, any treatment (understood as such any of the operations described in article 4.2/ of the RGPD) of the data collected by the FAMT in the framework of the provision of the public health service, is within the scope competence of this Authority based on the provisions of articles 156.a) of the Statute of Autonomy of Catalonia and 3.f) of Law 32/2010.

2.2. On the proven fact 1st, concerning data protection by design and by default.

In its statement of objections to the initiation agreement, the FAMT argued that in the description of the imputed conduct it had not been taken into account that, as they reported in the previous information, in the When defining the different profiles with access to patients' clinical history, not only the professional profile (doctor, nurse, etc.) is taken into consideration, but also the center and service from which it will be developed medical assistance. And he cited, by way of example, the following profiles: *"Mútua Terrassa University Hospital Doctor HUMT". "ÀPTIMA Hospital Doctor, "HUMT Outpatient Doctor" and "ÀPTIMA Consulting Doctor".* In accordance with the above, the accused entity considered that *"technical and organizational measures have indeed been applied when defining the different access permissions to the information in the patients' clinical history",* measures that complement with the *"control of the legitimacy of all the accesses made"* since said accesses *"are duly recorded, and this Access Register allows full traceability of these accesses, which are the subject of a monthly audit to verify that respond to a legitimate purpose".*

In this regard, in the resolution proposal the instructor pointed out that, certainly, in the description of the access profiles that had been collected in the 1st point of the proven facts section of the initiation agreement, it was not specified that the aforementioned profiles were defined, not only based on the professional category, but also taking into account the center and service from which the health care would be provided. This last element, however, was not included in the imputed fact because, as stated in the actions, the element of the profile that determines which data can be accessed by the people who provide service to Grup Mútua de Terrassa is that linked to the professional category (doctor, nurse, etc.) and not that of the center from which said service is provided. In other words, a person, for example, with the professional category of "doctor", can access the same information regardless of whether they provide the service at the FAMT or ÀPTIMA (and therefore have an associated profile such as those described in previous paragraph). In short, what is imputed here is not the lack of different access profiles to the patients' clinical history, but the fact that, as the clinical history database is configured

of the patients of the Terrassa Mutual Group and the permission policy, the professionals who provide service at ÀPTIMA can access the medical history of all patients of the Terrassa Mutual Group (and, therefore, of the FAMT), regardless what was the scheme - public, private or both - of the benefit received. Thus, and as the FAMT stated in the previous information, professionals with the access profile *"Physician Àptima Hospital"* and *"Physician Àptima Practices", "operationally have the possibility to access the clinical histories of all the patients included in this database, regardless of who is the guarantor of the medical services provided (CatSalut, a mutual fund or insurance company contracted by the patient, or if the cost of these is assumed by the patient himself). With respect to the rest of the user profiles (nurses, nursing assistants, administrative staff, etc.), the powers of access to patient data also do not depend on the guarantor who assumes the cost of the assistance, but on the specific needs to carry out their functions within the entity".*

In accordance with this, in this procedure it has been established that a doctor with the access profile *"Physician Àptima"* - Dra. (...)- was able to access the medical history of the reporting person, and was able to consult the health data that had been collected by the FAMT as part of the health care provided in the public health system - without no more restriction than that derived from her professional category of doctor. Thus, as the FAMT has admitted in this procedure, the ÀPTIMA doctor profile has associated privileges/permissions that allow him to access the clinical histories of all the people who have been treated by the FAMT , and therefore, be able to access the health data that have been collected for the care provided in the framework of public health. And this possibility of access, as recognized by the FAMT, also applies to other professionals (nursing, administrative staff), since *"the powers of access to patient data do not depend on the guarantor who assumes the cost of assistance".*

Well, this potential in the access available to the professionals who provide service to ÀPTIMA in the private healthcare system, to access the health data incorporated in the clinical history, when these have been collected by the FAMT in the if of care linked to the provision of public health services, it would not be justified at all for any care reason (as will be analyzed in detail later) and clashes head-on with data protection by design and by default, obligation collected in article 25 of the RGPD, and particularly, for what is of interest here, in its section 2 *["The person responsible for the treatment will apply the appropriate technical and organizational measures with the aim of guaranteeing that, by default, the data will only be the object of treatment personal that are necessary for each of the specific purposes of the treatment. This obligation will apply to the amount of personal data collected, the extent of its treatment, its retention period and its accessibility. Such measures will guarantee in particular that, by default, the personal data are not accessible, without the intervention of the person, to an indeterminate number of natural persons"].*

At this point it is not superfluous to point out that the National Security Scheme, approved by Royal Decree 3/2010, and applicable, in accordance with the first additional provision of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (in

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

hereinafter, LOPDGDD) to the FAMT due to the agreement signed with the Catalan Health Service by which it adheres to the Integral Health System for public use, provides in its article 19, relating to *"safety by default",* the Next:

"Systems must be designed and configured in such a way as to guarantee security by default:

a) The system will provide the minimum functionality required for the organization to reach its objectives.
b) The functions of operation, administration and registration of activity will be the minimum necessary, and it will be ensured that they are only accessible by the persons, or from locations or equipment, authorized, being able to demand in their case time restrictions and authorized access points.
c) In an operating system, the functions that are not of interest, are unnecessary and, even those that are inadequate for the purpose pursued, will be eliminated or deactivated, by means of the control of the configuration.
d) The ordinary use of the system must be simple and safe, so that an unsafe use requires a conscious act on the part of the user".

Finally, in its statement of objections to the initiation agreement, the FAMT pointed out as an element to be taken into account in its favor the fact of having implemented periodic audits in order to verify the lawfulness of access to the clinical histories. Well, as the instructor indicated in the proposal, although the fact that the FAMT has implemented periodic audits in order to verify the lawfulness of access to clinical histories must be positively assessed, it must be said that this measure - useful and enforceable - what would allow the entity to act reactively in the face of eventual improper access; when precisely what is intended from data protection by design and by default is that, within the possibilities offered by the technique, it becomes technically impossible to carry out data treatments that are a priori known to be unjustified. It is, in short, to address privacy proactively and preventively, in order to prevent eventual threats from materializing. In this sense, it must be borne in mind that linking access permissions to a profile that are not necessary, as in the case that has been analyzed here, only increases the risks of the confidentiality of the information.

In its statement of objections to the proposal, the FAMT states that it was in 2003 when *the "electronic clinical history system shared between the Group's healthcare entities" was implemented ,* and that prior to its implementation analyzed *"in a proactive way, the implications and risks for the interested parties that could arise from this treatment",* entrusting this analysis to external auditors which was embodied in single reports issued in 2002 and 2003, and on the basis of which *"all the risk-minimizing measures that were feasible at the time from a technical and organizational point of view"* have been applied in subsequent years . Finally, the FAMT adds that the fact that the medical professional cannot access all the information obtained from a patient, both within the framework of the provision of public and private health services, would mean that in practice a patient could *" conceal relevant medical information from the professional attending you in any of these centers, and therefore,*

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

the medical professional could not apply his lex artis (...) to safeguard the physical integrity of the patient (...)".

This Authority does not question the FAMT's interest in complying with data protection regulations, but the point is that, in accordance with what has been set out in this section and is considered proven, the entity does not has implemented to date the appropriate measures required by the RGPD and which would guarantee data protection by design and by default. Thus, there is no doubt that the potential of all the professionals who work at ÀPTIMA to access indiscriminately the health data of all the people served by Grup Mútua de Terrassa cannot be justified for healthcare reasons. And, as has been said, this potential does nothing more than exponentially increase the risks of information.

Regarding the eventual concealment of information by the patient alleged by the FAMT, a fact that in his opinion would prevent the medical professional from applying his *lex artis* to safeguard the physical integrity of the patient; it is worth saying that this possible concealment does not constitute any legal basis that can enable the treatment and access to all the patient's medical information obtained within the framework of the public medical benefit. The decision to hide information by the patient would be a freely made decision, so it would be the patient who would have to bear the consequences of having hidden it; this without prejudice to the health professional, precisely on the basis of the *lex artis,* practicing the appropriate medical tests in order to ensure adequate and safe medical assistance.

2.3. On the 2nd proven fact, relating to the lack of legality in the processing of the health data of the reporting person.

We remind you here that the treatment that is considered illegal is the consultation by people who provided service to ÀPTIMA (cited in point 2 of the proven facts section) - some workers from said entity, others from companies external-, of the data of the reporting person that had been collected by the FAMT as part of a public provision of health services. It is worth saying that this access was facilitated by FAMT's lack of implementation of appropriate technical measures, as explained above.

In its statement of objections to the initiation agreement, the FAMT asserted that there would be several legal bases that would have legitimized this treatment: a) provision of explicit consent (art. 6.1.a/ RGPD), that the person here the complainant would have provided on two occasions, on 09/05/2016 and 07/23/2019, by signing the documents entitled *"Consent for the use of personal data"* and *"Informed consent - Consent for the use of personal data" ,* respectively; b) the need to execute a contract (6.1.b/ RGPD), the need to comply with a legal obligation (art. 6.1.c/ RGPD); and the need to protect the vital interests of the person concerned (art. 6.1.d/ RGPD). The FAMT added that, in addition to the previous legal bases, in this case *"the following exceptions to the prohibition of processing special category data are applicable": a) "the interested party has given his express and written consent in the form prior to the processing of the data (art. 9.2 letter RGPD), b) The processing is necessary for the medical diagnosis and/ or the provision of healthcare assistance or treatment, in*

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

virtue of a contract with a healthcare professional subject to the duty of professional secrecy (art. 9.2 letter hi 9.3 RGPD); and, c) The treatment is necessary to protect the vital interests of the interested party) [(...) in the event that the interested party is not able, physically or legally, to give their consent), the addition is of the Authority] (art.9.2 letter c RPGD)". It is worth saying, however, that the FAMT, in the statement of objections to the proposal, only cites as the legal basis for the treatment the one provided for in article 6.1.b) in connection with the exception in article 9.2 .h) of the RGPD.

The FAMT also emphasized, both in its allegations in the initiation agreement and in the resolution proposal, the fact that FAMT and ÀPTIMA are joint owners of the patient file of the Terrassa Mutual Group which, as he said, includes the clinical histories of all the people treated by any of the companies in the aforementioned Group.

With respect to this allegation, it should first be emphasized that the fact that FAMT i ÀPTIMA are companies of the same group and "joint owners" of the file in question, it does not mean that they are different companies, each with its own legal personality. Thus, the FAMT would be the entity responsible for the data collected as part of care provided within the framework of the public health system, so that if any of the other companies in the Group had access to said data - how would the case we are dealing with - we would be dealing with a communication of data and therefore a new treatment different from the collection of the data by the person in charge. So, what needs to be analyzed is whether this communication of data has a legal basis that legitimizes it.

The RGPD requires, in order to carry out special category data processing - such as health data -, on the one hand, the concurrence of one of the legal bases provided for in article 6.1 of the RGPD and, on the other hand, cumulatively, that one of the exceptions provided for in article 9.2 of the RGPD is granted that lifts the general prohibition of processing data of this nature. To the above it should be added that article 9.2 of the LOPDGDD requires that the treatments provided for by letters g), h) ii) of article 9.2 of the RGPD, must be covered by a rule with range law. Therefore, it is appropriate to address in the first place whether the treatment that is the subject of controversy would be legitimated by any of the legal bases provided for in article 6 of the RGPD, since if this were not the case it would no longer be necessary to analyze the eventual concurrence of one of the exceptions listed in article 9.2 of the same rule.

As has been said, the FAMT invoked in its statement of objections to the initiation agreement several legal bases different from consent, those specified in letters b), c) or d) of article 6.1 of l 'RGPD and which, according to their understanding, legitimized the treatment; although in the statement of objections to the proposal, the justification for the treatment is based on the basis provided for in article 6.1.b) of the RGPD. All the legal bases invoked by the FAMT in this procedure are then analyzed.

2.3.1.- Regarding the need for processing for the execution of a contract (art. 6.1.b/ GDPR)

The FAMT argued in its statement of objections to the initiation agreement that *"for the fulfillment of the task of providing health care arranged with the patient with the*

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

medical professional of Aptima, it was necessary to obtain all the information possible to carry out, safely, the surgery entrusted to this professional". In its statement of objections to the proposal, the FAMT insists on this last argument stating that *"the medical professional must necessarily know all the health circumstances that could affect the physical integrity of the patient".*

In this regard, it is worth saying, as established by Group 29 in its Opinion 6/2014, that to assess the "need" or not of a treatment, it must be taken into consideration if other means are available invasive to serve the same purpose, and not only that: to assess this "necessity" related to the execution of a contract it is also essential to determine whether or not the contract can be executed without this specific treatment. Well, this would not be the case we are dealing with here, in which the medical professional could have carried out the relevant medical tests to carry out the intervention with complete safety, without having to access the clinical data obtained as part of a medical care provided by the public health system. It is true that the computer application allowed this direct access to the information, but, as has been said, this deficiency - which is also the object of imputation in this procedure - cannot become the justification or necessity of the access

2.3.2.- Regarding the need for treatment in compliance with a legal obligation applicable to the person responsible for the treatment. (art. 6.1.c/ RGPD)

In its statement of objections to the initiation agreement, the FAMT invoked in relation to this legal basis the health legislation, among other things and for what is of interest here, article 9.1 of the Catalan Law 21/ 2000, of December 29, on the rights of information concerning the health and autonomy of the patient, and the clinical documentation, which establishes that the maximum integration of the clinical documentation of each patient must be sought, integration that *" it must be done, at least, in the scope of each center, where there must be a unique clinical history for each patient";* article 14.1 of Law 41/2002, of November 14, basic regulation of patient autonomy and rights and obligations in the field of clinical information and documentation, which defines the clinical history as the set of documents relating to care processes of each patient in order to obtain the maximum possible integration of the clinical documentation of each patient, at least, in the scope of each center; and, article 16 of the same Basic Law 41/2002, which refers in its section 1 to the clinical history as *the "instrument intended fundamentally to guarantee adequate assistance to the patient",* and in its section 2 to the need that each center establish *"methods that enable access to the clinical history of each patient at all times by the professionals who assist them".*

With regard to the clinical history unit, it is of interest to quote the Court's judgment here Supreme Court dated 10/20/2009 which was pronounced in the following terms:

"As for the clinical history, it is true that the arts. 14 et siguientes of the Patient Autonomy Law favor "the maximum possible integration of the clinical documentation of each patient" in order to achieve adequate health care. Perhaps this justifies speaking, as the contested sentence does, of a principle of unity of the clinical history. I say this, yes

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

I must immediately point out that this integration of the clinical history, tending to avoid the dispersion of health information about each patient, has as beneficiary the patient himself. The initial paragraph of art. 16 of the Patient Autonomy Law is crystal clear in this regard:

"The clinical history is an instrument primarily intended to guarantee adequate assistance to the patient." Clinical records should not have a unitary character, as the contested sentence claims, to facilitate their mission to occupational risk prevention associations, and even less so to employers. Certainly, they allow providing better health care; but this improvement is not justified by the saving of effort for third parties (health personnel, administration, employers, etc.), but by the well-being of the patient. This point is of crucial importance, because information on people's health is part of the object protected by the fundamental right to privacy, as clarified, among others, by the Constitutional Court ruling 196/2004. Hence, any exception to the confidentiality that weighs on said information can only be justified by the benefit it brings to the patient himself or, as the case may be, by inescapable and superior requirements of the general interest duly weighted, which in no way can consist of a functioning

more agile than the occupational risk prevention mutuals. So it is that art. 18 of the Patient Autonomy Law only confers the right of access to the clinical history to the patient, not to third parties; and the subsequent art. 19 of that same legal text obliges to establish "a mechanism for active and diligent custody of clinical records".

According to this interpretation, and as explained by the instructor in the resolution proposal, the principle of unity of the clinical history for each center and the desideratum established in the aforementioned health regulations to provide adequate assistance to the patient would not justify the transfer of information between companies indiscriminately, no matter how much they are part of the same Group. Interpreting it in another way would lead to validating the communication of medical data between public and private centers without any other justification than to provide adequate assistance, resulting in a lack of control on the part of the affected people over who, why and in under what circumstances your data is being processed, which is completely contrary to data protection regulations.

To the above it should be added that the shared clinical history implemented in Catalonia (in accordance with the additional provision of Law 21/2000 and article 56 of Law 16/2003 of "Cohesion and Quality of the National Health System") provides the exchange of medical information between health centers in the public care network (publicly owned and privately owned centers that are part of SISCAT), but no rule currently contemplates access or interoperability with databases or files of clinical histories of private health centers that do not provide medical services agreed with public health.

2.3.3.- Regarding the need for treatment to protect the vital interests of the person concerned (art. 6.1.d/ RGPD)

In relation to this legal basis, the FAMT argued in its statement of objections to the initiation agreement that *"the consultation carried out by Dra. (...) of your patient's health data*

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

it was necessary for the preservation of her vital interests, as a surgical intervention had been scheduled, which had to be carried out with the greatest safety for the patient".

In relation to the legal basis 6.1.d) of the RGPD that was already analyzed by the instructor in the proposal, it must be said that recital 46 establishes the following: *"El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger an essential interest for the life of the person concerned or that of another natural person. In principle, personal data only they must be treated on the basis of the vital interest of another physical person when the treatment cannot be manifestly based on a different legal basis. Certain types of treatment may respond both to important reasons of public interest and to the vital interests of the interested party, such as when treatment is necessary for humanitarian purposes, including the control of epidemics and their spread, or in situations of humanitarian emergency, on all in case of natural or man-made disasters".*

Group 29 in the aforementioned opinion 6/2014, determined that a restrictive interpretation of this provision must be made, and, in the line that was finally embodied in the transcribed recital, established that *"it is reasonable to assume that in situations in which there is the possibility and the need to request a valid consent, the consent must, of course, be requested whenever possible".*

Therefore, based on this, this legal basis cannot be accepted as legitimating the aforementioned treatment either.

2.3.4.- Regarding consent (6.1.a/ RGPD)

Discarded the legal bases contained in article 6.1, letters b), c) and d) of the RGPD, it is now necessary to focus on the analysis of consent as a legitimizing legal basis for the treatment, a basis that was also invoked by the FAMT in its submissions to the initiation agreement.

The FAMT defended that the complainant had given his explicit consent on two occasions, on 05/09/2016 and 23/07/2019, by signing the documents entitled *"Consent for the use of personal data"* and *"Informed consent – Consent to the use of personal data",* respectively. It stated that *"in the first paragraph of both informative documents, the co-ownership of the patient file between FAMT, ÀPTIMA, and the Vallparadís Foundation is expressly and transparently stated. These documents also include the rest of the conditions for the treatment of the patient's personal data, among them, the purpose of the treatment and the transfer to third parties: specifically, the first of the consents expressly states that "the recipients of the data will be the estates public or private entities outside the Group's entities that, due to material needs or legal imperative, must access their data for the correct provision of healthcare" and that "by signing this document, the patient of Mútua de Terrassa MPS and/ or ÀPTIMA CENTER CLÍNIC, gives its consent so that the data that are expressly necessary are transferred to the entity with which the patient has arranged the provision of medical-health and social services, with the aim to access the payment of the cost of the assistance provided». Therefore, it is contemplated*

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

expressly the circumstance of data processing by both FAMT and ÀPTIMA, regardless of who assumes the cost of the medical treatment (a public entity or an insurance company" [the emphasis is by FAMT].

As the instructor indicated, at this point it should be remembered that the processing of health data based on consent requires the provision of explicit consent (art. 6.1.a/ and art. 9.2.a/ of the RGPD).

Of the two forms referred to by the FAMT, through which the complainant here would, according to his understanding, have given his explicit consent, only the document *"Consent for the use of personal data" will be* analyzed that the person making the complaint sign on 09/05/2016. The other consent document invoked by the FAMT, which is also signed by the person making the complaint, could not constitute - in the event that it met the requirements - a valid legal basis for this particular treatment since, as evidenced by the instructor, this was signed on 23/07/2019, i.e. after the date on which the treatment attributed here was carried out /(...)/2019). That consent must be given before the processing activity begins is a requirement that is clearly inferred from the wording of articles 6.1.a) and 9.2.a) of the RGPD *("the interested party gives his consent for the treatment").* Accordingly, it will be the form of 09/05/2016 that will be analyzed in the light of the provisions of the RGPD.

Section 11 of article 4 of the RGPD defines consent as *"any manifestation of free will, specific, informed and unequivocal by which the interested party accepts, either by means of a statement or a clear affirmative action, the treatment of data personal that concern him".*

It is appropriate here to focus on two of the conditions that this manifestation of will must fulfill: that it be specific and unequivocal.

Guidelines 5/2020 of the European Data Protection Committee (EDPB) on consent, regarding the need for the expression of will to be specific, states the following:

"Article 6, section 1, letter a), confirms that the consent of the interested party for the treatment of their data must be given "for one or several specific purposes" and that an interested party can choose with respect to each of these purposes. The requirement that the consent must be "specific" aims to guarantee a level of control and transparency for the interested party. This requirement has not been modified by the RGPD and is still closely linked to the "informed" consent requirement. At the same time, it must be interpreted in line with the requirement of "dissociation" to obtain "free" consent. In short, to comply with the "specific" character, the person responsible for the treatment must apply:

and the specification of the end as a guarantee against the deviation of the use,
ii the dissociation in requests for consent, and
iii a clear separation between information related to obtaining consent for data processing activities and information related to other issues".

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

And on the unequivocal condition that must be given in the consent given, the CEPD document itself determines that:

"75. The RGPD clearly states that consent requires a statement from the interested party or a clear affirmative action, which means that consent must always be given through an action or statement. It must be evident that the interested party has given consent to a specific data processing operation.
76. Article 2, letter h), of Directive 95/46/CE described consent as "any expression of will, free, specific and informed, through which the interested party consents to the treatment of personal data that concerns him". Article 4, section 11, of the RGPD develops this definition by clarifying that valid consent requires an unequivocal manifestation of said will by means of a statement or a clear affirmative action in line with the previous guidance published by GT29.

77. A "clear affirmative action" means that the interested party must have acted deliberately to give consent to that particular treatment. Recital 32 provides additional guidance on this point."

Well, it must be said that the document in question, signed by the person reporting on 05/09/2016, and which has been partially transcribed in this same section, absolutely contains a consent that meets the conditions of specific and unequivocal with regard to the treatment consisting in the communication of data by the FAMT to ÀPTIMA which is, ultimately and as has been explained, the treatment subject to imputation. And this because there are no different treatments (on the one hand, the processing of data by the FAMT within the framework of public healthcare provision; and on the other hand, the communication of data by the FAMT to others companies of the Group), nor the specific purposes of each of these possible treatments, nor is there a clear separation between information related to obtaining consent for data processing activities and information related to other issues (as contained in the CEPD guidelines transcribed above).

Nor can it be considered that the consent was explicit, a requirement required by article 9.2.a) of the RGPD with regard to the treatment of special categories of data, such as health data. And this because the terms in which the document is written would prevent the affected person from clearly and expressly expressing his will as to what would be the specific treatments he would be accepting by signing said document.

In accordance with what has been explained, it is considered that the controversial treatment is not legitimated by any of the legal bases alleged by the FAMT in the framework of this procedure.

2.4. On the 3rd proven fact, relating to the violation of the principle of limitation of purpose.

In relation to this imputation, the FAMT argued the following in its statement of objections to the initiation agreement: *"We understand that (...) Mútua de Terrassa has complied*

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

enough with the duty to inform about the specific, explicit and legitimate purpose of the treatment of the data collected from the patient". In this sense they explained that *"in the informed consent of 09/05/16, shared by FAMT, ÀPTIMA: The purpose is the "providing of the medical-health service and the formalization of the clinical history, and the corresponding administrative and invoicing tasks that correspond, being able to be recipients of the data public and private entities that have to access the data for the correct provision of medical-sanitary assistance",* and that *"in the informed consent of 07/23/19 , it is reported even more explicitly (...). The treatment of health data for the purpose of providing health care cannot be considered incompatible, depending on the circumstance of who assumes the costs of the health care received by the patient (either the patient himself, or a private insurance entity arranged by this, or the Public Health System. Affirming this implies violating the principle of uniqueness of the Clinical History within a health center".*

In its statement of objections to the proposed resolution, the accused entity, on the one hand, asserts *that "the APDCAT is not competent to rule on a treatment carried out by ÀPTIMA, a company that it is not within its scope of action";* and, on the other hand, he reiterates what he already stated in his previous statement of objections, in the sense that *"health treatment cannot be considered incompatible with the purpose of providing health care, depending on the circumstance of who assumes the costs of this healthcare provision",* since there is no legal regulation that contemplates *"a different purpose according to who assumes the cost of healthcare",* indicating in this respect that not even the *"Protection Guide of Data for patients and people using health services"* published by the APDCAT, in the section in which *"the different purposes are broken down (...) it mentions (...) the criterion on which it has been based the APDCAT's sanction proposal (...) consisting of a bifurcation of the assistance purpose, depending on who assumes the cost of this assistance".*

Before entering into the analysis of the principle of limitation of the purpose it is necessary to clarify, first, that as has been said before, the only document that will be taken into consideration here will be the one that was signed by the person making the complaint before that the FAMT carried out the treatment subject to controversy in (...)/2019. And second, it is also necessary to demonstrate that the transcription made by the FAMT in its letter of allegations to the agreement initiating the consent document of 09/05/2016 is incorrect, since the literal wording of the document, when refers to the recipients cited by the FAMT in this allegation, is as follows: *"In the same way, the recipients of the data will also be public and private entities other than the entities of the Group mentioned above that, due to material needs or legal imperative, must access the data for the correct provision of medical-sanitary assistance" (the* emphasis is by the Authority) . In any case, it must be emphasized that purpose and recipients are two of the elements - distinct and non-interchangeable - of which the interested person must be informed prior to the collection of their data. Therefore, what will be analyzed here is the purpose for which the data of the affected person was collected and its eventual incompatibility with subsequent treatments, and not the eventual recipients of the information.

It should also be noted that the FAMT is right when it states that ÀPTIMA is an entity that provides non-contracted private services and that therefore it would not fall within the scope of its activities

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

authority But what is being analyzed here is not the action carried out by ÀPTIMA, but the use made by the FAMT of the data that this entity collects in the framework of public healthcare, and specifically, if its subsequent processing fits the purpose for which they were collected
this data; and this is the competence of this Authority.

Having clarified this, it is then necessary to analyze whether the treatment described in the 3rd of the proven facts is respectful of the principle of purpose limitation.

Article 5.1 of the RGPD describes in letter b) what the purpose limitation principle consists of, in the following terms:

"1. The personal data will be: (...)
b) collected for specific, explicit and legitimate purposes, and will not be subsequently treated in a manner incompatible with said purposes; in accordance with article 89, section 1, the further processing of personal data for archival purposes in the public interest, scientific and historical research purposes or statistical purposes will not be considered incompatible with the initial purposes ("limitation of the purpose") .

For its part, article 6 -relating to the legality of the treatment- establishes the following in section 4:

"4. When the treatment for a purpose other than that for which the personal data was collected is not based on the consent of the interested party or on the Law of the Union or of the Member States that constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives indicated in article 23, paragraph 1, the person responsible for the treatment, in order to determine whether the treatment with another purpose is compatible with the purpose for which the personal data was initially collected, will take into account, among other things: a) any relationship between the purposes for which the personal data have been collected and the purposes of the subsequent treatment provided; b) the context in which the personal data have been collected, in particular with regard to the relationship between the interested parties and the controller; c) the nature of personal data, in particular when special categories of personal data are treated, in accordance with article 9, or personal data relating to criminal convictions and infractions, in accordance with article 10;

d) the possible consequences for the interested parties of the planned subsequent treatment; e) the existence of adequate guarantees, which may include encryption or pseudonymization.

And recital (50), also referring to the purpose of the treatment, provides that:

The processing of personal data for purposes different from those for which they were initially collected must only be allowed when it is compatible with the purposes of their initial collection. In such a case, a separate legal basis is not required, other than the one that allowed the personal data to be obtained. If the treatment is necessary for the fulfillment of a

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

mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment, the tasks and purposes for which the subsequent treatment should be considered compatible and lawful can be determined and specified in accordance with Union Law or the member states. Subsequent processing operations for archival purposes in the public interest, scientific and historical research purposes or statistical purposes must be considered compatible lawful processing operations. The legal basis established in the Law of the Union or Member States for data processing
Personal data can also serve as a legal basis for further processing. In order to determine whether the purpose of the subsequent treatment is compatible with the purpose of the initial collection of personal data, the person responsible for the treatment, after having fulfilled all the requirements for the authorization of the original treatment, must take into account, among other things , any relationship between these purposes and the purposes of the intended further treatment, the context in which the data were collected, in particular the reasonable expectations of the interested party 4.5.2016 ES Diario Oficial de la Unión Europea L 119/9 based on their relationship with the person responsible for its subsequent use, the nature of the personal data, the consequences for the interested parties of the planned subsequent treatment and the existence of adequate guarantees both in the original treatment operation and in the planned subsequent treatment operation.
If the interested party gives his consent or the treatment is based on the Law of the Union or of the Member States which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the person responsible must be authorized for the further processing of personal data, regardless of the compatibility of the purposes. (…)"

In view of the precepts transcribed, it is first necessary to determine for what purpose the data of the reporting person were collected by the FAMT, and specifically, by the CAP (...). As has been said, the FAMT collects the data of CAP users - among them the reporting person - as part of the public health provision. The purpose of the treatment in this context is intimately linked with the legal basis that legitimizes the treatment of health data in the context of public health, which is established in article 6.1.e) *("el tratamiento es necesario for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment"),* in connection with the exception provided for in article 9.1.h) ii) of the RGPD. It is therefore clear that the data of the reporting person were collected in order to provide medical assistance within the public health system.

Well, these data of the reporting person collected in the framework of a public health benefit, as has been proven, were treated by ÀPTIMA as part of a private benefit, therefore, with a different purpose for the which were initially collected.

Having established this, and in accordance with the regulations, it is then necessary to analyze whether this treatment for a different purpose could be based on the provision of consent. The answer to this question must be negative since, as analyzed in point 2.3.4 above, according to the wording of the document signed by the person reporting on 09/05/2016, it cannot consider

that the affected person gives their consent - which must be explicit, as it concerns health data - for the treatment that is the subject of controversy.

If the processing of the data is carried out for a different purpose for which the data were initially collected, and is not based on the consent of the person concerned, in accordance with the provisions of article 6.4 of the RGPD , the person in charge must prove that the treatment for this different purpose is compatible with the purpose that justified the initial collection of the data. Well, the reasons put forward by the FAMT in order to substantiate the compatibility of the treatment based on the *"uniqueness of the clinical history of the health center",* cannot be accepted for the reasons already set out in point 2.3.2. precedent, and which are reproduced here. And even more, it is not possible to defend a possible compatibility in the case at hand, if one of the criteria defined in article 6.4 of the RGPD is taken into account and which must be used to carry out this "compatibility test", and is the one referred to *"the context in which the personal data have been collected, in particular with regard to the relationship between the interested parties and the person responsible for the treatment".* Indeed, given the context in which the data were collected - public health provision - the affected person could not foresee at all that their data will be used in the provision of a private health service.

To the above it should be added that this further processing of the data for a different purpose than that for which it was initially collected would not be legitimated by any other legal basis, in accordance with what has been set out in section 2.3 precedent

To conclude with this analysis of the purpose, add that the fact that among the purposes detailed in the *"Data Protection Guide for patients and users of health services"* of the APDCAT - to which the FAMT to its allegations - the purposes of medical assistance do not differ depending on who provides the service (public or private health), does not at all invalidate what has been said so far, and this because, first, it is a guide and not a mandatory legal rule; and, secondly, because the list that is made there is by way of example, which is quite obvious since it would be impossible to capture in a single closed list all the purposes for which the data can be processed. And proof of this, of the merely illustrative nature of these lists, is the document that FAMT itself mentions in its allegations drawn up by the AEPD, in which they only mention the purpose of care and medical research by regarding the treatment of health data.

2.5. On the 4th proven fact, relating to the violation of the principle of loyalty.

The FAMT stated in its statement of objections to the initiation agreement that *"aware of the complexity that can be posed, in terms of personal data protection, by the fact that the same entity in the care field develops its activity under various legal entities, depending on whether it is an activity financed by the Public Health or a private activity, Mútua de Terrassa has informed all its users of the conditions for processing their data, either personally, through the documents information that has been proven to have been delivered to the complainant on the day, and also through other means of dissemination, such as Mútua de Terrassa's web pages. The erroneous "reasonable" expectation on which the proposal is based*

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

sanction, we understand that this is a subjective argument, which is not based on any objective evidence other than the complaint submitted by a patient (...)". These same arguments are reiterated by the FAMT in its statement of objections to the proposal.

The principle of loyalty is included in article 5.1.a) of the RGPD in the following terms: *"Personal data will be treated in a lawful, fair and transparent manner in relation to the interested party".* The principle of loyalty is not expressly defined as such in the RGPD, although its recital (60) alludes to the same determinant that *"the principles of fair and transparent treatment require that the interested party be informed of the existence of the treatment operation and its purposes. The person responsible for the treatment must provide the interested party with all the additional information necessary to guarantee a fair and transparent treatment, given the specific circumstances and context in which the personal data is treated (…)".*

The idea of loyalty is closely linked to the requirement of good faith, a principle enshrined in our positive law in article 117-7 of Law 29/2002, of December 30, of the Civil Code of Catalonia, which determines that *"in private legal relationships, the requirements of good faith and honesty in dealings must always be observed";* and the same rule, in its statement of reasons, refers to said principle in the following terms: *"article 111-7 incorporates a rule on good faith because in the tradition of Catalan law, along the lines of continental law of which it is a part, is a general principle which, therefore, cannot be limited to the contractual area. It also refers to the honesty of the deals, as a differentiated concept, because, in accordance with the most recent evolution of European private law, it wants to highlight the objective aspect, independent of the knowledge or ignorance of each of the subjects of the legal relationship".*

This principle of good faith is also enshrined in article 7.1 of the Civil Code of the Spanish State: *"Los derechos must be exercised in accordance with the requirements of good faith"*

The Supreme Court, in its judgment of 05/21/1982, approaches the interpretation of the principle of good faith in the following way: *"the "principio de la buena fe", como límite al exercise de los derechos jetivos, requires the fixation of its significance and scope, and in this sense already TS 1.ª S 29 Ene.1965 establishes a series of typical assumptions, whose concurrence authorizes, "in general terms", to admit they contradict said principle, specifying that it is lacking in the good fe when it goes "against the result of one's own acts, an equivocal act is carried out to benefit intentionally from its dubious meaning, or a legal appearance is created to contradict it afterwards to the detriment of those who put their trust in it""*

And the Supreme Court itself, in a more recent judgment of 09/17/2010, pronounced itself in the following terms: *"As stated in judgment number 988/2005, of 22 December hacienda suyas las palabras of the of 19/2005, of January 19: (...) good faith does not refer to subjective good faith (belief, psychological situation), but to objective (honest, just behavior), which is referred to in article 7 of the Code, which enshrines as a norm the general principle of law of that number, with what implies a legal mandate with organizing social effectiveness (...)"*

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

In view of all of the above, it can be said that the principle of loyalty requires the person in charge to have an honest attitude in relation to the treatment of personal data, in the sense of not carrying out treatments that - not being provided for by the regulations -, the people affected cannot reasonably wait in accordance with the context and circumstances of its collection, therefore, not carrying out treatments betraying the trust that the affected person has placed in the person responsible for the treatment.

Certainly, the assessment of the loyalty or good faith of an action, of the "expected conduct", must be measured, not from the subjectivity of the specific person affected, but with external objective standards, that is to say, what the average citizen would expect in the same context and situation. And this is precisely the reference that the Authority took into account when making this imputation: any person who goes to the CAP (as the complainant did) in order to be treated in public health care, could not at all expect that the health data collected in this context could be consulted by a company of the same Group that provides private healthcare.

The fact that the document provided to the citizen mentions the "co-ownership of the file" between several companies does not alter this reasoning, taking into account, in addition, as explained above, neither the information provided to the affected person clearly contemplates this possible treatment.

In accordance with all the above, the allegations made by the FAMT in this procedure cannot be admitted.

3. In relation to the fact described in point 1 of the proven facts section, it is necessary to refer to article 25 of the RGPD, which provides the following in relation to data protection by design and by default:

> *"2. The controller will apply the appropriate technical and organizational measures to ensure that, by default, only the personal data that are necessary for each of the specific purposes of the treatment are processed. This obligation will apply to the amount of personal data collected, the extent of its treatment, its retention period and its accessibility. Such measures will guarantee in particular that, by default, the personal data are not accessible, without the intervention of the person, to an indeterminate number of natural persons".*

During the processing of this procedure, the fact described in point 1 of the proven facts section, which is considered constitutive of the violation provided for in article 83.4.a) of the RGPD, which typifies as such the violation of *"the obligations of the responsible and of the manager",* among which is the collection in article 25 of the RGPD transcribed above, referring to the protection of data by design and by default.

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

> *"The lack of adoption of technical and organizational measures that are appropriate to guarantee that, by default, only the personal data necessary for each of the specific purposes of the treatment are processed, in accordance with what is required by article 25.2 of Regulation (EU) 2016/679"*

4. With regard to the fact described in point 2 of the proven facts section, regarding lawfulness in the processing of health data, it is necessary to refer to articles 5.1.a), 6 and 9 of the RGPD, which provide the next:

Article 5.1.a) of the RGPD:

> *"1. The personal data will be:*
> *(...)*
> *a) treated in a lawful, fair and transparent manner in relation to the interested party ("lawfulness, loyalty and transparency")".*

Article 6 of the RGPD:

> *"Lawfulness of the*
> *treatment 1. The treatment will only be lawful if at least one of the following conditions is met:*
> *a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes; b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures; c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment; d) the treatment is necessary to protect the vital interests of the interested party or another natural person; e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment;*
>
> *f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child.*
>
> *The provisions in letter f) of the first paragraph shall not apply to the processing carried out by public authorities in the exercise of their functions.*

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

Article 9 of the RGPD:

"Processing of special categories of personal data 1. The processing of personal data that reveals ethnic or racial origin, political opinions, religious or philosophical convictions, or trade union affiliation, and the processing of genetic data, targeted biometric data are prohibited to uniquely identify a natural person, data relating to health or data relating to the sexual life or sexual orientation of a natural person25.

2. Section 1 will not apply when one of the following circumstances applies: a) the interested party gives his explicit consent to the treatment of said personal data with one or more of the purposes specified, except when the Law of the Union or the Member States establish that the prohibition mentioned in section 1 cannot be lifted by the interested party; b) the treatment is necessary for the fulfillment of obligations and the exercise of specific rights of the person responsible for the treatment or of the interested party in the field of labor law and of social security and protection, to the extent that this is authorized by the Law of the Union of the Member States or a collective agreement in accordance with the Law of the Member States that establishes adequate guarantees of respect for the fundamental rights and interests of the interested party; c) the treatment is necessary to protect the vital interests of the interested party or another natural person, in the event that the interested party is not physically or legally able to give their consent; d) the treatment is carried out, within the scope of its legitimate activities and with due guarantees, by a foundation, an association or any other non-profit organization, whose purpose is political, philosophical, religious or trade union, provided that the treatment refers exclusively to current or former members of such organizations or persons who maintain regular contact with them in relation to their purposes and provided that personal data is not communicated outside of them without the consent of the interested parties; e) the treatment refers to personal data that the interested party has made manifestly public; f) the treatment is necessary for the formulation, exercise or defense of claims or when the courts act in the exercise of their judicial function; g) the treatment is necessary for reasons of an essential public interest, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish measures adequate and specific to protect the fundamental interests and rights of the interested party;

h) the treatment is necessary for the purposes of preventive or occupational medicine, evaluation of the worker's labor capacity, medical diagnosis, provision of assistance or treatment of a sanitary or social type, or management of the

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

systems and services of health and social assistance, on the basis of the Law of the Union or of the Member States or by virtue of a contract with a health professional and without prejudice to the conditions and guarantees contemplated in section 3; i) the treatment is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, or to guarantee high levels of quality and safety of health care and medicines or health products, on the basis of the Law of the Union or of the Member States that establishes appropriate and specific measures to protect the rights and freedoms of the interested party, in particular professional secrecy, j) the treatment is necessary for purposes of archiving in public interest , purposes of scientific or historical research or statistical purposes, in accordance with article 89, paragraph 1, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish appropriate and specific measures to protect the fundamental interests and rights of the interested party"

For its part, article 9 of the LOPDGDD provides the following regarding the treatment of special categories of data, among which health data is at the top:

"1. (...)
2. The data treatments provided for in letters g), h) ii) of article 9.2 of Regulation (EU) 2016/679 based on Spanish law must be covered by a rule with the rank of law, which may establish additional requirements regarding its security and confidentiality.
In particular, this rule can protect the processing of data in the field of health when this is required by the management of health and social assistance systems and services, public and private, or the execution of a contract insurance of which the affected person is a party".

In accordance with what has been stated, the fact collected in point 2 of the section on proven facts constitutes the violation provided for in article 83.5.a) of the RGPD, which typifies as such the violation of *"the basic principles for treatment, including the conditions for consent pursuant to articles 5, 6, 7 and 9 ",* among which the principle of legality is at the top.

The conduct addressed here has been included as a very serious infraction in article 72.1.e) of the LOPDGDD, in the following form:

"The processing of personal data of the categories referred to in article 9 of Regulation (EU) 2016/679, without any of the circumstances provided for in the aforementioned precept and article 9 of this Organic Law"

5. With regard to the fact described in point 3 of the proven facts section, referring to the principle of purpose limitation, it is necessary to refer to article 5.1.b) of the RGPD which provides the following:

> *"1. The personal data will be:*
> *(...)*
> *b) collected for specific, explicit and legitimate purposes, and will not be subsequently treated in a manner incompatible with said purposes; in accordance with article 89, section 1, the further processing of personal data for archival purposes in the public interest, scientific and historical research purposes or statistical purposes will not be considered incompatible with the initial purposes ("limitation of the purpose") ;*

For its part, article 6.4 of the RGPD provides the following:

> *"When the treatment for a purpose other than that for which the personal data was collected is not based on the consent of the interested party or on the Law of the Union or of the Member States that constitutes a necessary and proportionate measure in a democratic society for to safeguard the objectives indicated in article 23, paragraph 1, the person responsible for the treatment, in order to determine whether the treatment with another purpose is compatible with the purpose for which the personal data was initially collected, will take into account, among other things: a) any relationship between the purposes for which the personal data have been collected and the purposes of the subsequent treatment provided; b) the context in which the personal data have been collected, in particular with regard to the relationship between the interested parties and the controller;*
>
> *c) the nature of personal data, in particular when special categories of personal data are treated, in accordance with article 9, or personal data relating to criminal convictions and infractions, in accordance with article 10; d) the possible consequences for the interested parties of the planned subsequent treatment; e) the existence of adequate guarantees, which may include encryption or pseudonymization".*

During the processing of this procedure, the fact described in point 3 of the proven facts section, which is considered constitutive of the violation provided for in article 83.5.a) of the RGPD, already transcribed, has been duly proven to the 4th legal basis, and which typifies as such the violation, among others, of the principle of limitation of purpose

The conduct addressed here has been included as a very serious infraction in article 72.1.d) of the LOPDGDD, in the following form:

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

"The use of the data for a purpose that is not compatible with the purpose for which they were collected, without having the consent of the affected person or a legal basis for this"

6. With regard to the fact described in point 4 of the proven facts section, referring to the principle of loyalty, it is necessary to refer to article 5.1.a) of the RGPD already transcribed in the 4th legal basis.

In accordance with what has been stated, the fact collected in point 4 of the section on proven facts constitutes the infraction provided for in article 83.5.a) of the RGPD, also transcribed above and which typifies as such the violation, among others, of the principle of loyalty.

The conduct addressed here has been included as a very serious infraction in article 72.1.a) of the LOPDGDD, in the following form:

"The processing of personal data that violates the principles and guarantees established by Article 5 of Regulation (EU) 2016/679"

7. As the FAMT is a private law entity, the general penalty regime provided for in article 83 of the RGPD applies.

Article 83 of the RGPD foresees for the infractions provided for in its section 4, they are sanctioned with an administrative fine of 10,000,000 euros at the most, or in the case of a company, an equivalent amount to a maximum of 2% of the overall total annual business volume of the previous financial year, opting for the higher amount. For its part, section 5 of the same precept provides for the infractions provided for there to be sanctioned with administrative fines of 20,000 euros at the most, or in the case of a company, an amount equivalent to 4% at the most of the overall total annual business volume of the previous financial year, opting for the higher amount. This, without prejudice to the fact that, as an additional or substitute, the measures provided for in clauses a) ah) ij) of Article 58.2 RGPD may be applied.

In the present case, as explained by the instructor in the resolution proposal, it is considered that the conduct described in points 2, 3 and 4 of the section on proven facts, constitute a violation of the principles of legality, limitation of the purpose and loyalty, respectively, and all three provided as an infringement in article 83.5.a) of the RGPD, are closely linked, so that the infringement relating to the principle of limitation of purpose and loyalty would be subsumed by the relative infringement to the violation of the principle of legality.

Likewise, it is estimated that with regard to the infractions referred to above and the one described in the basis of 3rd right relating to the violation of data protection by design and by default, we would be faced with a case of ideal concurrence of infringements, given that although the accused entity has committed different infringements, there is a direct connection between the two, because the non-implementation of appropriate measures in accordance with data protection by design and by default has led to the violation of the other principles.

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

Article 29.5 of Law 40/2015, of October 1, on the legal regime of the public sector (hereafter, LRJSP), provides that *"When the commission of an infraction necessarily leads to the commission of another or others, only the penalty corresponding to the most serious offense committed must be imposed."*

In view of the above and the provisions of the aforementioned article 29.5 of the LRJSP, sanctions will be imposed only for the commission of the most serious infringement, that is to say, the one relating to the principle of legality.

With regard to the sanction to be imposed, first of all it must be said that the possibility of replacing the sanction of an administrative fine with the sanction of reprimand provided for in article 58.2.b) RGPD has been ruled out, in view of the concurrence of offenses committed, although, as stated, he will be punished only for the commission of an offence.

Once it is ruled out that the penalty of an administrative fine should be replaced by a warning, it is necessary to determine the amount of the administrative fine which, at the discretion of this Authority, must impose.

Article 83.2 of the RGPD determines the following, regarding the graduation of the amount of the administrative fine:

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

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

i) when the measures indicated in article 58, paragraph 2, have been previously ordered against the person in charge or the person in charge in relation to the same matter, the fulfillment of said measures;
j) adherence to codes of conduct under article 40 or certification mechanisms approved under article 42, and
k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as the financial benefits obtained or the losses avoided, directly or indirectly, through the infringement."

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

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

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

According to what is established in articles 83.2 RGPD and 76.2 LOPDGDD, and also in accordance with the principle of proportionality enshrined in article 29 of the LRJSP, as indicated by the instructor in the resolution proposal, a penalty of 60,000 euros should be imposed (sixty thousand euros).
This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

On the one hand, we appreciate the following circumstances that operate as mitigating criteria:

- FAMT's adherence to the code of conduct of the Catalan Hospitals Union (art. 83.2.j GDPR).

In contrast to the attenuating causes set out, a series of criteria from article 83.2 of the RGPD that operate in an aggravating sense also apply:

- The nature, gravity and duration of the infringement, taking into account the nature, scope and purpose of the treatment operation in question, as well as the number of interested persons affected (art. 83.2.a/). It is here in consideration that the lack of implementation of a security policy from the design can lead to a serious

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

problem of confidentiality of special categories of data that would potentially affect all people who are treated by the FAMT in the public health regime.

- The degree of responsibility of the person in charge or of the person in charge of the treatment, taking into account the technical or organizational measures that have been applied under the provisions of articles 25 and 32 of the RGPD (art. 83.2.c/ of the RGPD).
- The previous infringements committed (art. 83.2.e/ of the RGPD), since it is known that the FAMT has previously been sanctioned for various violations of the regulations on the protection of personal data (sanctioning procedures no. PS 18/2012, PS 13/2020 and PS 27/2020).
- The categories of personal data affected by the infringement (art. 83.2.g/ RGPD), in this case, special categories of data (data relating to health).
- The link between FAMT's activity and the processing of personal data (art. 83.2.k of the RGPD and 76.2.b/ of the LOPDGDD).

8. Faced with the finding of the violations provided for in article 83 of the RGPD, article 21.3 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, empowers the director of the Authority so that the resolution declaring the infringement establishes the appropriate measures so that its effects cease or are corrected, in line with what is also provided for in art. 58.2 of the RGPD, in addition to imposing the corresponding fine. By virtue of this power, and with regard to the conduct described in point 1 of the proven facts section, the FAMT is required because as soon as possible, and in any case within the maximum period of one month from the day after the notification of this resolution, proceed to implement the relevant technical and organizational measures by design and by default, in order to prevent the people who provide services to the Mutual Group of Terrassa under the private healthcare system can access, without the explicit consent of the affected persons, their health data collected as part of public healthcare.

Once the corrective measure described has been adopted within the period indicated, within the next 10 days the FAMT must inform the Authority, without prejudice to the inspection powers of this Authority to carry out the verifications corresponding

With regard to the conduct described in points 2nd, 3rd and 4th of the section on proven facts, as they are specific facts already accomplished, corrective measures should not be required.

For all this, I resolve:

1. To impose on the Mutual Aid Foundation of Terrassa the sanction consisting of a fine of 60,000.- euros (sixty thousand euros), as responsible for an infringement classified in article 83.5.a), in relation to the article 5.1.a) of the RGPD regarding the principle of lawfulness (infringement that subsumes the violations of the principles of limitation of purpose and loyalty, given their link); in ideal competition with the infringement provided for in article 83.4.a) in relation to article 25 regarding data protection by design and by default; all of this in accordance with what is stated in the 7th law foundation.

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

2. Require the Mutual Aid Foundation of Terrassa to adopt the corrective measures indicated in the 8th legal basis and accredit before this Authority the actions taken to comply with them.

3. Notify this resolution to the Mutual Aid Foundation of Terrassa.

4. Order that the resolution be published on the Authority's website (apdcat.gencat.cat), in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with the provisions of article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

The director,