□ File No.: PS/00281/2022

RESOLUTION OF SANCTIONING PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and in

based on the following

BACKGROUND

FIRST: On 03/23 and 24/2021, a claim from A.A.A. is received, hereinafter,

the claimant) against SECURITAS DIREC ESPAÑA, S.A. with NIF A26106013

(hereinafter, the claimed party).

In it, it indicates that in procedure TD/01593/2017, the Agency issued a

resolution as follows: "Securitas must provide access to the appellant the

information on the servers (...) related to the records and signals sent

by the alarm equipment (...), as well as the existing copies of the records

contained in the internal memory of the alarm between 11/26 and 12/13 of the year

2015". This resolution was appealed by Securitas Direct S.A. and confirmed by the

National audience.

This procedure for the exercise of rights occurs as a consequence of the fact that the

claimant had previously exercised his right of access to the respondent on

04/07/2017: “regarding all the information on the Securitas servers

Direct relative to the records and signals sent by the alarm equipment installed in”

their property, “as well as existing copies of the records contained in the

internal memory of the alarm between November 26 and December 18 of the

year 2015 (before and after the robbery there were other security incidents that should be

also clarify)", "given that they have the unequivocal classification of data

personal”. The information to which access is requested makes direct or

indirectly to events and occurrences (entries, exits, movements, jumps of alarm, activation and deactivation of the alarm by certain user, etc.)

occurred inside my home, from which it can be inferred, directly or

indirectly, acts or behaviors related to myself, other people

of my family or even third parties authorized to access the home”.

In relation to this right of access, the defendant replied on 05/11/2017 that

“the records contained in the alarm do not fall into the data category

personal", according to a copy of document 5 that he provides.

Not agreeing with the answer given by the security company, the claimant

mante files a claim with the Agency on 06/28/2017, in which, among other

issues, indicates that on the afternoon of 12/4/2015, he discovered, upon accessing his home,

who had suffered a robbery and found "the alarm center" destroyed, without having been

warned, receiving only a call from the security company of that same morning.

morning in which they indicated that there were connection problems. In the text of the re-

complaint filed with the Agency, the claimant states that the claimant "is

has refused to clarify the circumstances of the intrusion into our home or to

reveal the cause of the malfunctioning alarm system, ensure

checking that the system worked correctly", being the clients the ones who had to

telephone the security company to inform them that the alarm center that

had installed had been destroyed by thieves.

The aforementioned claim was resolved on 01/2/2018 in the appeal for replacement of the

procedure for the exercise of rights TD/01593/2017, estimating the appeal and requiring within a period that the right be met.

The defendant appealed the resolution before the National Court (AN), which in the Judgment of the Administrative Litigation Chamber, first section, of 07/23/2019, appeal 146/2018, dismissed his claim.

The judgment of the National Court was appealed before the Supreme Court in appeal, admitted for processing on 05/29/2020, appeal 78/2020, however, the claimed withdrew from it.

The claimant alludes in his new claim, that he has once again requested access on 02/2/2021 and received a response from the defendant of 02/23/2021, which highlights:

1) Responds: "in compliance, first of the resolution of the appeal for reversal RR 779/2017 of the AEPD and the judgment of the National Court.", "attaching as document 1, a list of "logs associated with said alarm system that are data of a personal nature”.

Document 1 starts:

“In order to understand the configuration of the table that we have prepared with the logs which are personal data…”, and explains the meanings of the three columns.

The provided Excel table of logs contains in the first column the date/s and time/s in which the log, or logs, is generated. They are not arranged chronologically. beginning by 5/12/2015. Only one log appears chronologically defined between two dates, 5/12/2015 18:38:10 and 20:15:17. It comprises a total of 94 lines of logs, plus that of the period, so it is unknown how many there would be in total.

The generation date or dates of the logs are correlated or grouped with the “log name/nomenclature”, and with a basic description such as “Signal information”, “CRA Action” (alarm receiving center), “tests and verifications mandatory as part of the maintenance of the installation“.

In the last column, with "extended description of the log", which according to the defendant contains a description of the meaning of the log, in some cases the key N/A appears, associated with a nomenclature, for example "CRA action Skip voicemail", “operator gets to talk to contact”, or “the contacts the operator gets to Securitas tries to locate, they don't answer”.

In others, it is not specified either by indicating: "a message is left on voice mail".

In some log it refers to "contact", without identifying or specifying which contact refers, as "contact does not remember the password to prove the identity and

close the incident”, or “the contacts that the Securitas operator tries to locate no answer”, “operator manages to speak with contact”.

It is observed that there are logs that include: "automatically generated code and randomly by the system for the security guard to deactivate the alarm"-, name: “High priority central”, or another name of the log: “tests and obligatory verifications as part of the maintenance of the installation” connected with “extended name: “the technician performs regulatory checks to ensure the proper functioning of the system. At the request of the client you can modify some parameter of the system itself.

The defendant points out that: "To simplify the information there are different dates and hours associated with a log, and this is because we have grouped the dates and hours in which they were generated in Mr.'s system.”

The claimant considers that it has not been answered satisfactorily, because:

-Access to the information on the servers has been filtered/reduced by

Securitas to the logs that they consider personal data, an issue that does not corresponds to do.

-"The table provided with schematic information does not satisfy the right of exercised access. For example, on page one, in the nomenclature column "CRA Action", it is stated "different generic actions of the operator Securitas human resources in the event of a specific incident (e.g. authorization of the speak/listen; call to the different listed contacts; internal comments on relation to the information transmitted to you by contacts)" but without any indication of What kind of action/information has been registered regarding the incidents listed, which prevents the applicant for the right of access, understand and analyze said logs, which is the ultimate goal of this access request.”

-"Finally, the response from Securitas is non-existent regarding the second part of the access request contained in the resolution: "existing copies of the records contained in the internal memory of the alarm", "not having indicated in any moment if those copies do not exist or access is not given because they do not consider that they are not "personal data logs".

With the presentation of the claim by the claimant, he states that he has not correctly attended to his right and with the elapsed time he is caused helplessness

SECOND: The claim gave rise to the AEPD resolving on 09/17/2021 a procedure for lack of attention to the exercise of rights (arts. 15 to 22 of the GDPR), TD/00167/2021, in which in the process of transferring the claim for Resolution (E/4382/2021), the defendant, stated on 05/19/2021:

-"The claimant of the right of access did not request at any time after the firmness of the sentence its execution or that the resolution of the Agency that was appealed in the same”.

Confirms receipt of the claimant's letter requesting the exercise of the right of access, to which he "responded with receipt of 03/03/2021."

-Consider that not all the logs that record the signals of the alarm equipment, as well as the contents in the internal memory of the same can be considered that contain personal data, and that was inferred from the verbatim of the sentence: "Among the information on the servers..., if there are data of a personnel of the owner of such contracted alarm". For this reason, it commissioned a report in 2020 to a legal office that established it so, to differentiate them, which does not contribute, but "makes available to the AEPD".

It indicates that, as a result of this exercise and this report, it currently has a "management protocol".

It explains its position based on said Report, which is summarized below.

Based on the legal concept of personal data, in order to determine if the information has the status of personal data because it relates to a natural person identified or identifiable, it will be necessary to analyze the affectation that the information produces in it.

"Regarding its content, the information must assume an attribute of any kind predicable directly from the interested party in question, there being a direct relationship between-three attribute and person.

Regarding its purpose, the processing of information must have as its purpose the co-knowledge of the mentioned attribute of that person.

As for its effects. the information must refer to aspects that affect the interest

resed as a consequence of the aforementioned attribute.”

In the explanatory term of what personal data is, it is defined by "all information

information about a natural person", it starts from when it refers to her, "and as consequence, at the moment in which the information provided is not derived or linked

directly to the physical person, but to objects that belong to him or are under his control.

creep, only indirectly can the information be considered to refer to that

person and provided that it allows inferring data referring to that natural person and

not to the object itself. Therefore, information about an object will only have the

consideration of personal data when a connection or link is established between the

object and the affected party in order to generate information about said person”.

The defendant has differentiated two categories in which the

different logs.

In the first category would be the logs that they consider do not imply

processing of personal data, which may include:

“- those in which information about an interested party is not collected through

said logs that individualize it from the rest of the population,

-The knowledge of said information is not intended in order to carry out a

analyzing or influencing behavior, and

- your rights and freedoms are not affected.“

List the categories of logs that would be found in this scenario:

1) "Emission of signals of a purely technical nature for communication between the dispositive as part of the verification protocol of its correct functioning or

to register a technical failure.

2) Registration of informative signals in relation to, among others, the version of the system,

model or category of the installed device.

3) Descriptive record of internal and technical procedures before a specific event.

4) Recording of technical signals in relation to device configurations

that do not provide information about the interested party or their habits but simply

reflected in calibrations of the Securitas systems for their correct functioning.

I lie.

5) Statistical information about the devices.“

It also alludes that "said logs" could contain information on technical processes.

Internal data of the defendant whose disclosure to third parties could imply dissemination of sec-

trade creds. For this purpose, it mentions recital 63 of the GDPR, as legitimate

maker of "discriminating the information that can be provided to the person who exercises

the access."

In a second category would be the logs that do consider that they imply treatment.

processing of personal data, to the extent that:

- "They collect information about an interested party and its intrinsic characteristics,

-Knowledge of said information is sought to analyze it or influence its behavior.

treatment,

-Your rights and freedoms are affected."

Adding or specifying that "not all logs in this category would imply the processing of

data processing of the contract holders", but rather "could imply the processing

processing of personal data of third parties”. In this category would be included

the following logs.”

1) “Processes carried out by Securitas operators or technicians, who occasionally

These may be considered personal data of a third party other than the client of Securitas”

2) "The active interactions of the user himself -or third parties- with the physical systems

or through the mobile application.

3) "Passive interactions of the user or of third parties that may provide information

tion in relation to their way of acting at a given moment or their availability

in front of an event.

4) Records of identifiers of the interested parties that are contained in the logs, such

such as first and last name or email addresses.”

5) Images or data in connection with an intrusion or sabotage. In this sense, it is pre-

ciso indicate that if the intruder is captured by the security camera, to the extent that

that said person is identifiable as a result of the image obtained, we would find ourselves

before a personal data of the same.”

6) Pulsations entering codes that determine a particular situation of the interesado.

7) Configurations of the user himself that determine a knowledge of his tastes

or behavior patterns.

It states that the access response provided to the claimant contained the logs

which are personal data that affect the client, being "excluded the

technical or that affect third parties”.

-They add that they have sent an email to the claimant on 05/18/2021, provide a copy of do-

document 4 in which they refer to what was already sent on 02/26/2021, received by the claimant

keep on 3/3/2021.

-State that the causes that have motivated the original incidence of the claim

are due to the fact that "not all the logs generated by an alarm system are data from

personal character".

-On 06/07/2021, the Director of the AEPD agreed to "the agreement of admi-

processing, and the initiation of a procedure for the exercise of rights of the articles

15 to 22 GDPR", procedure TD/00167/2021.

-At the heart of said procedure, the defendant, (...), states:

a) In relation to the content of the "internal memory of the alarm installed in the

address of the claimant", this generated logs until 11/27/2021, 20:09, time and date

in which the intrusion into the home occurred - as you already know - during which

said alarm system was completely disabled. As of that date, no

could generate more logs of any kind. Therefore, in the time frame between 11/26 and

12/18/2015, the internal memory could only generate logs on 11/26 and 27/2015, and after

the analysis of the logs generated in the internal memory of the alarm, only consisted of a

log generated in that time frame, which was included in the response given to the claim

kept on 02/23/2021. They provide document 1, which is the table with columns of the access

so that the claimant was given on that date, in which it appears marked in green

fluorescent that log, and in which you can read:

"11/27/2015 20:09:47/HIGH PRIORITY CENTRAL PANEL/Automatically generated code and

randomly by the system for the security guard to deactivate the alarm".

They consider that they have complied with the right of access.

Already within the processing of TD/00167/2021, on 06/23/2021, the claimant was sent Keep the copy of the response given by the defendant, and dated 07/16/2021, the re-plaintiff stated:

-On the one hand, the information must be provided in a transparent and intelligible. “The incomplete list of logs provided by Securitas Direct does not allow to this party to understand in a transparent and intelligible manner the information contained in your servers regarding the operation of the existing alarm system in my home".

On the other hand, it indicates that what the defendant has done has been to prepare a list of logs filtered by the contracted law firm, differentiating those that may be considered to contain personal data of those that do not. Add that this differentiation does not correspond to the one claimed and states that "the Hearing Nacional considered that all the logs are personal data and from this it deduces that access has been incomplete.”

-Considers that giving access to the log is not fulfilled, but to "the information contained in the servers relative to the registers and signals of the alarm equipment installed in his property". It would consider that the resolution is fulfilled when "it has been given access to all existing information on the servers in relation to the operation of the alarm installed in my home”. "The information operating on the servers in relation to the operation of the alarm installed in my home goes much further of these logs to which the Securitas Direct access right is intended, and includes any information in the form of text, images, alphanumeric etc. existing on its servers that is related to the records and signals of the alarm installed in my home.

-Considers that the refusal of the defendant to provide access to the information

operating on its servers may be due to the fact that it intends to evade its responsibilities

individuals in relation to the damages caused in this robbery and “delay and

make it as difficult as possible to properly investigate the reasons for

poor functioning of the alarm system installed in my home”.

-About the response provided to the log of the internal memory of the alarm,

considers implausible the assertion that the alarm center generated logs up to

20:09 on 11/27/2015, when the intrusion occurred and said system was disabled,

since that supposed intrusion actually refers to a jump of the alarm of the

perimeter detector of the garage door, room that is physically located

separated from the home and that it was not affected by the theft and estimates that the

intrusion into the home occurred on a date after 11/27, since "if the central

alarm was” destroyed, Securitas could hardly have disconnected

remotely the same.

It emphasizes that the request for access to the records contained in the memory is

They refer to both "the destroyed alarm center and the one that was installed in my home

on 12/5/2015 and that it continued to generate signals and records”.

On 09/17/2021, the procedure for exercising rights was resolved,

agreeing to estimate the claim and granting a term to address the right. The

resolution was appealed for replacement on 10/18/2021, resolving on 10/27/2021 its dismissal, and the defendant was notified electronically on 10/28/2021.

It is interesting to highlight from it, that the defendant, appellant, stated:

-The resolution of the procedure for the exercise of rights considers addressing the right, but it does not determine the information that should be considered personal data, it does not Give reasons for your conclusion. Nor does it establish “that the All the logs generated by the installed alarm system have effectively the consideration of personal data”. It only details what the claimed, that "it does not meet all of what was requested, specifying the reason", "without determine if that totality will incorporate information that has nothing to do with the data protection regulations”.

"Nor is the claimant's claim that the SAN of 07/23/2019 will indicate that all the information or all the logs generated by the alarm system have to be considered personal data.", since the sentence on its grounds of the fourth right, indicates that "within the logs there are personal data", which which allows us to conclude that "not all of them should be considered as such". Esteem that "it is not possible to exercise the right of access to personal data with respect to information that at no time can be considered personal data”, and adds that the AEPD in the different resolutions relapsed in this case has not defined that information contains data that must be subject to the regulations for the protection of data, "it is evident that" the defendant can define what information the mentioned character”.

"Neither the judgment of the AN nor the resolution have defined what information it contains data that should be considered subject to the data protection regulations”, therefore that they will be the ones who have to delimit it.

Reproduces part of opinion 4/2017 on the concept of personal data adopted on 06/20, WP 136:

“Sometimes, the information provided by the data refers not so much to people as objects. These objects usually belong to someone, or may be under the influence of or exert influence over a person or may have a certain physical or geographical proximity to people or other objects. In those cases, only indirectly can the information be considered to refer to those people or objects.

A similar analysis can be applied when the data refer in the first instance to processes or events, such as the operation of a machine when it is human intervention is necessary. Under certain circumstances, this information it can also be considered information “about” a person.”

It shows its disagreement with the content of the resolution, which indicates "since the claimant is the holder of the alarm contract, the regulations are applicable on Data Protection regarding the right to access the logs on the operation of the alarm installed on your property”.

"In addition to recitals 26 to 28 for the conceptualization of the data personal, not only have this condition the information that allows the identification of the interested party, but also that which allows their identification.

For these purposes, the explanatory report of convention 223 of the Council of Europe on 10/10/2018 tries to clarify the content of individualization or singularization in these terms:

“This individualization could be done, for example, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, game devices etc.) on the basis of a number identification, a pseudonym, biometric or genetic data, location data, an IP address or other identifier. The use of a pseudonym or any digital identifier/digital identity does not give rise to the anonymization of the data, since that the interested party can still be identifiable or individualized. Therefore, the data pseudonyms should be considered personal data and are covered by the provisions of the agreement."

“The defendant considers that the information included in the alarm system may not refer to an interested party, nor to its characteristics, attributes or behaviors, nor even least affect it in any other way or allow the inference of information regarding the same. Indeed, in general, these logs would consist of information that They only refer to the communication between data systems merely operational and technical that have nothing to do with an interested party or are linked to that of no way, and only some of these logs could allow obtaining information about the physical person who owns the alarm”. Give three examples related in the five cases in which in his report he considered "no data personal”, specifically:

In 1), "the battery level of the device, disconnection from the network, inhibition, etc." It was about the "Issuance of signals of a purely technical communication nature between the devices as part of the verification protocol of their correct operation or to record a technical failure”.

In 3), "waiting times processed before an event, collection and description of the event, capture process and making available to the operators of the images or sounds, modification of internal parameters, transfer of the event to a operator etc. It referred to “Descriptive record of internal procedures and technicians before a specific event".

In 5) "number of photos captured, activated devices, quality of responses of the devices, number of disconnections, etc.). He meant "Information statistics about devices.

He also gives examples of what he has previously classified as "data from personal character", such as:

In 1), "Securitas Direct personnel whose activity is registered in the own logs". It referred to: "Processes carried out by operators or technicians of Securitas, which can sometimes be considered personal data of a third party different from the Securitas client"

In 3), "the Securitas Direct operator initiates a call and it is answered, or not by the user, the security code is requested and the user includes it correctly or not, no movements are recorded for a period of time determined in the monitored area, etc. He was referring to: "Passive interactions of the user or third parties who may provide information in relation to their form to act at a certain moment or their availability in the face of an event.

In 6) "panic button or inclusion of the alarm deactivation code under duress", referred to: Images or data in connection with an intrusion or sabotage. In

In this sense, it is necessary to indicate that if the intruder is captured by the security camera, security, to the extent that said person is identifiable from the image obtained, we would find ourselves before a personal data of the same."

In point 76 “the different (...)s that he uses, times of said (...)s, configurations Personal information about device volume, language, selected parameters on air quality or designation of names of users and zones, etc.”, which relates to: "Settings of the user himself that determine a knowledge of their tastes or behavior patterns.

If all generated logs were given access, anyone would have the right to said type of access due to the fact of having contracted the installation of a alarm, with internal technical operations being "publicly accessible" unrelated to a person and that reveal substantial information about the effectiveness and operation of the commercialized systems, being able to violate the law of secrets business 1/2019 of 02/20 and relates it to recital 63 of the GDPR.”

Regarding the claimant's expression that it is not possible to understand the logs (action CRA...) points out that the format to satisfy the right of access was to comply with with the provisions of article 12 of the GDPR "in a concise, transparent, intelligible and easily accessible, with clear and simple language" and that "the information is is listed in the table attached to the brief of 02/23/2021", and that "even those data is registered in a technical way and little intelligible for any person not well-versed in the terminology of alarm systems, and even in the terminology itself internal Securitas, so that its reading would not reveal the information that if incorporated into the form sent to the interested party”. He states that he “carried out a adaptation of the logs to a clear and simple language to attend to the law”. indicates They have no objection to delivering the information in "lines of code formats", although compliance with the requirements would satisfy the right to a lesser extent required by the GDPR.

THIRD: On 11/4/2021, the claimant submits a document in which states that the provisions of resolution TD/00167/2021 are still not being complied with.

On 12/2/2021, the AEPD sent a letter to the defendant, reiterating the request of the compliance with the resolution, granting a term and warning of the consequences of its breach.

On 12/21/2021, the defendant submits a document in which she states "satisfying compliance with the resolution" and provide a copy of the letter of 12/14/2021 and documents letter sent to the claimant. It states: “A job has been carried out again exhaustive to provide D.xxx with any records and signals sent by the alarm equipment that could be linked to the performance, behavior or its characteristics, excluding information that is not considered tion of personal data as it is exclusively technical information that also affects the legitimate interest of Securitas Direct in the confidentiality of its secrets business.”

In relation to the records contained in the internal memory of the alarm between the days November 26 and December 18, 2015, the (micro card or chip) of the Securitas Direct alarm systems record and store information from events with a technical origin and from events originating in the interaction of devices installed in customers' homes. In the case of equipment installed to D. xxx the records of the internal memory reach up to the moment in which it was rendered useless and all records collected prior to that At the moment, they are events of a technical nature, so it is not personal information.”

It accompanies the records in "excel" sheets with the chronological ordering of logs by date.

date and time and more informative columns such as event", "event (...)", "Zone", "***COLUMNA.3", "***COLUMN.4". "***COLUMN.1""area", "time of (...)" to name only valaughs.

The description column contains short descriptive terms that are not common.

understandable, for example, EVENT: word whose specific meaning is not understandable

, the same as in "event (...)", and in general in all columns.

According to the defendant, it is the "literal transcription, in the format in which it is included in the

SD systems from the records and signals sent by the alarm equipment."

FOURTH: On 05/07/2022, the claimant submits a document in which he states

that the response of the defendant persists in classifying the logs that are data

personal of those who do not, when it does not correspond, reiterating that the matter has already been

ruled by the AN. He points out that the right continues to be ignored for years, returning

to the origins of the judgment of the AN. The picture is unintelligible, the expression of the

description is imprecise, the print is very small, most of the logs correspond to

the technical intervention to replace the destroyed alarm the day after the theft:

12/5/2015, therefore "completely useless and irrelevant". "They continue without

provide the information that motivates the exercise of the right of access, which is not

other than clarifying the circumstances of the robbery in my home and settling possible

responsibilities", and that "you need to know what happened with the alarm".

It requests, "the forced execution of its resolution be agreed...", without prejudice to the

"opening of a disciplinary procedure".

FIFTH: On 06/8/2022, the Director of the AEPD agreed:

"INITIATE SANCTION PROCEDURE against SECURITAS DIRECT ESPAÑA, S.A., with NIF A26106013, for the violation of article 58.2 c) of the GDPR, typified in art. 83.6 of the aforementioned GDPR and 72.1.m) of the LOPDGDD."

"For the purposes specified in the art. 64.2 b) of Law 39/2015, of 1/10, on Procedure Common Administrative System of Public Administrations (LPACAP, hereinafter), the sanction that could correspond would be 50,000 euros, without prejudice to what results from the instruction."

Said initiation agreement was duly notified, granting the defendant a term to make allegations

SIXTH: On 07/06/2022, the defendant made the following allegations:

1) He reiterates that during the year 2020, they commissioned a law firm to report, of which they provide a copy in DOCUMENT 1 (signature date 01/29/2021) (already mentions the same before in the response to the transfer of the claim of 05/19/2021, content supra regarding TD/00167/2021), on the "application of the concept of personal data to the signals or logs generated by the alarm systems", with the object of whether all or part of them have the status of personal data to the effects of the application of substantive regulations, and secondarily as

2) Document that for the future allows to attend the requests of exercise of rights.

The report has on the cover: "confidential", unaware if it would reach all of its content.

The report based on the historical definitions in the personal data legislation, considers that the GDPR introduces an extensive concept, considering that "not only The information that allows the identification of the interested party will have this condition, but also the one that allows its "singularization", even when it was not possible to know directly or indirectly to the person to whom the data refers.

It alludes to Convention 108 of the Council of Europe, of 01/28/1981, on the protection of people in relation to the automated processing of their personal data, in the wording resulting from the reform operated by Agreement 223, of the Council of Europe, of October 10, 2018 (hereinafter, by the name commonly accepted "108+ Agreement") establishes in its article 2 a) that for the purposes of the Convention, personal data means "any information about a natural person identified or identifiable" and in relation to the concept of identifiable person, following the same line established in recital 26 of the GDPR, indicates the paragraph §18 of its explanatory report: “The notion of "identifiable" refers not only to the civil or legal identity of the individual as such, but also to what he can allow "individualize" or single out (and therefore allow to treat differently) a person from others. This "individualization" could be done, for example, referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, biometric or genetic data,

location data, an IP address or other identifier. The use of a pseudonym or any digital identifier / digital identity does not give rise to the anonymization of the data, since the data subject can still be identifiable or individualized. Therefore, the pseudonymous data should be considered personal data and is covered by the provisions of the Convention. The quality of the applied pseudonymization techniques should be duly taken into account when assessing the adequacy of safeguards implemented to mitigate risks to stakeholders.”

It follows that said concept is characterized by the necessary concurrence of four essential elements:

-Personal data is, in any case, information.

-This information must refer to a certain person since it must be about the same.

-The person to whom the information refers must be a natural person, remaining excluded from the concept of personal data are legal persons or entities without legal personality.

-The person must be identified or identifiable in the broad sense established by the recital 26 of the GDPR and paragraph 18 of the agreement 108 + that identify the concepts “that identifies” and identifiability, singularization and individualization.”

He mentions various jurisprudence of the most noteworthy cases on the concept of personal data from the European Union.

It considers that in order to determine, in accordance with the jurisprudence of the CJEU, whether a information has the status of personal data because it refers to (or deals with) a natural person identified or identifiable, it will be necessary to analyze the affectation that the information produces in it:

 Regarding its content, that is, the information must assume an attribute, so any kind, predicable directly from the interested party in question, there being a direct relationship between said attribute and said person. In this way, the information must appear linked to the interested party, excluding the concept of personal data that information that is not linked to a characteristic or activity of the former.

 Regarding its purpose, that is, the processing of information must have as its object the knowledge of the mentioned attribute predicable directly from that person, the purpose of the treatment being linked to the analysis of said attribute.

 Regarding its effects, that is, the information must refer to aspects that

affect the interested party precisely as a consequence of the aforementioned attribute. Are

measures may vary in their intensity (e.g. from the mere fact of

contact him until a profiling is carried out and decisions are made that

significantly affect).”

It also analyzes several sentences handed down in Spain on the concept and scope

of personal data and the analysis of the concept of personal data of Opinion 4/2007

on the concept of personal data, adopted by GT29 (document WP136, from

06/20/2007).

It is indicated in the Opinion: "a piece of information refers to a person if it refers to his

identity, characteristics or behavior or if that information is used to

determine or influence the way in which it is treated or evaluated”.

"A consequence of the foregoing will be that at the moment in which the information

provided does not derive or is directly linked to the physical person but to objects

that belong to him or are under his influence, can only indirectly be considered

that the information refers to that person and provided that it allows inferring

data referring to that natural person and not to the object itself.", cites example 5 "value of

a house" that refers to the application of the data protection regulations according to the

use of that information.

“The value of a home is information about an object. Clearly, the rules on data protection will not apply when that information is used solely to illustrate the level of housing prices in a certain area. However, under certain circumstances, that information must also be considered as personal data. In effect, the home is an asset of your owner and, as such, will be taken into account, for example, when calculating the taxes to be paid by that person. In this context, it is unquestionable that such information should be considered as personal data”.

“The Working Group has previously addressed the question of when it can information is considered to be "about" a person. Within the framework of his discussions on data protection issues raised by labels RFID, the Working Group noted that a "data refers to a person if it does reference to his identity, his characteristics or his behavior or if that information is used to determine or influence the way in which it is treated or evaluates». Taking into account the cases mentioned above, and following the same line of reasoning, it could be affirmed that in order to consider that the data are "about" a person there must be an element "contained" or an element "purpose", or a "result" element.

The "content" element is present in those cases where - in accordance with the that a society tends to generally and vulgarly understand by the word "on" - is provides information about a specific person, regardless of any purpose that may be harbored by the data controller or a third party, or the repercussion of that information on the interested party. Information is "about" a person when it "refers" to that person, which should be evaluated taking into account all the circumstances surrounding the case. By For example, the results of a medical analysis clearly refer to the patient, or the information contained in the file of a company under the name of certain client clearly refers to him: In the same way, the information contained in an RFID tag or a barcode embedded in the document identity of a certain person refers to that person, as in the future passports that will incorporate an RFID microprocessor.

The presence of an element "purpose" may also be what determines that the information to be "about" a certain person. It can be considered that element "purpose" exists when the data is used or is likely to be used, taking into account all the circumstances surrounding the specific case, with the purpose of evaluating, treating in a certain way or influencing the situation or the behavior of a person."

Based on this, the defendant considers that "in order to consider that" information is “about” a person must be found in at least one of the following three assumptions or circumstances:

1. "Content": that is, that the information refers directly to a person concrete physics. If this circumstance occurs, it will be irrelevant what the purpose is. of the person in charge of the treatment or of a third party recipient of the information or that repercussion will have the treatment of this information in the interested party.

2. "Purpose": the information collected, although it does not refer directly to a natural person, is used or is likely to be used for the purpose of evaluating, treating in a certain way or influence a person's situation or behaviour.

3. "Result": even assuming that none of the situations occur

above, information will be "about" a person when its use has repercussions on

the rights and interests of the same, being able to be treated differently from

other people as a result of the processing of such information.”

The defendant states that:

- "Therefore, information about an object will only be considered as

personal data when a connection or link is established between the object and the

affected (particularly, but not necessarily, its owner) in order to

generate information about said person or promote an action on his part.

The defendant states that: "Once the concept of personal data has been analyzed from

legal, doctrinal and jurisprudential perspectives, it is now necessary to analyze the application

of the mentioned concept to the logs generated by the alarm systems of

Securitas Direct, in order to determine which of them will have the status of "data

personal", with the consequent application in relation to them of the regulations

of data protection.”

“To carry out the analysis and qualification of the logs provided by Securitas Direct

As personal data, the following aspects have been taken into consideration:

to. It must be information, in any known format or form that

effectively imply the actual existence of data.

b. Said information must refer to a specific natural person, so the

The information contained in the logs must, at least, be found in one of the

following situations:

- Is directly linked to a specific individual, in such a way that

provide direct information about their way of acting, their mental characteristics

or physical, your preferences, your abilities or any other pattern of behavior that

can be directly attributed to it; either

- Can be used to evaluate or influence an individual in any way

determined or in his conduct; either

- Can directly affect the rights and interests of an individual

certain.

-"The information included in an alarm system may not refer to an interested party

nor to its characteristics, attributes or behaviors, nor even less affect it in any way.

any other way or allow the inference of information related to it. In

effect, in general, the aforementioned logs will consist of information that

They only refer to the communication between data systems merely

operational and technical that have nothing to do with an interested party, nor are they linked to it in any way.

no way and only some of these logs could allow information to be obtained

on the physical person who owns the alarm."

Based on these elements, two fundamental categories have been differentiated in

where the various logs provided by Securitas Direct could be found,

to. "Logs that do not imply processing of personal data". Reiterate the reasons and the

categories that he exhibited on 05/19/2021.

-Provides the differentiation in the same document 1:

An Annex I, which includes the specific "study" of the different logs that the security systems

Securitas generated in connection with the provision of its services to the claimant. Gave-

Cho Annex I contains, in turn, two different tables, grouping those lines of log

belonging to the claimant not considered as personal data (table I) (p. 23 to

30/105) and those that would have that consideration, in view of the analysis carried out carried out throughout the Report (table II), (p. 30/105).

In Annex II, the "general analysis and without specific application to an interested party" is attached

specifically, of the consideration as personal data of the generic log lines that

can normally be used in Securitas Direct systems during the development of its activity."

-Regarding Annex I, "given the amount of information provided, in relation to

with the logs", we have proceeded to identify them (both for table I and table II) by means of

you three columns:

1. In the first one, "date of the log line", the "dates and times

concrete appearance". It is appreciated that various dates and times can be grouped

2. In the second, the "name of the information" is included.

3. The following is: "extended description", "made up of both the information provided

by Securitas Direct during the various meetings held, as well as the

documents and tables received and the rest of the explanatory columns that are contained

in the log itself."

The defendant continues that: "Next, the" assessment of the

character of personal data of each of the logs" by including two co-

additional columns:

b. "In the fourth column, we proceed to assess whether the information contained in the line

particular log file allows Securitas Direct to collect information about the Claimant or

a third party, or analyze and cause an impact on their behavior", under the denomination

tion of: “linking, directly or through inference, to conduct or information

insult of a natural person”.

It is observed that they contain terms, such as operator, client, authorized user, con-

tacts designated by this, interested applicant of the right.

c. The last column specifies whether the log line can be considered, starting from

everything indicated, as personal data or not, with the literal Is it considered personal data?

No, in all those of table I, while table II, in "Is it considered personal data"?

nal?” figure "Yes", and a column is added: "It is likely to be provided

in response to the exercise of the right of access of the interested party?, appearing in some

In our cases: yes, and in other different annotations, since "lines of

log that could be considered personal data but refer to third parties

interested parties other than the Complainant himself and, it should be remembered, the request for access

exclusively allows the Claimant to have access to the personal data that

on his person deals with Securitas and not those on other natural persons.”

In table I, "Information not considered personal data in relation to the request for

analyzed access” (23 to 30), highlight:

- In three descriptors figure - "Linking directly or through inference, to

conduct or information of a natural person": “There is no direct link

with information of the interested party to the extent that these are personal communications

periodic machine-machine device status checks”, all with:

“extended description: Signals sent by the alarm that correspond to the state

of operation of the devices”, which can respond in: “name of

information:

In one case: “Superv Photo PIR RADIO, RADIO REPEATER, RADIO VOLUMETRIC”,

other: “radio repeater superv” and “radio volumetric superv”

-- - "Link directly or through inference, to a behavior or information of a natural person": "There is no direct link with information of the interresed to the extent that this log line does not collect information about the data subject.

nor is it intended to analyze or impact your behavior, it simply

allows an internal Securitas Direct process in relation to an initial alarm signal.

ma", and in "extended description": "Before the initial alarm signal, a time is given

type of margin in case it is a mistake or forgetfulness on the part of the user when not

deactivate the alarm.", "name of the information: trust wait 35 seconds

for a possible disconnection".

--- "Linking directly or through inference, to a behavior or information

of a natural person": "Information of a technical nature from Securitas Direct. In the meextent in which direct information about an attribute of the interested party is not transferred nor

Securitas Direct intends to analyze a pattern of conduct or to influence it in an al-

none, the information provided by the analyzed log line should not be considered

as personal data", "extended description: Detection of lack of electrical current

in the device", "name of the information: electric current-auto".

--- "Linking directly or through inference, to a behavior or information

of a natural person": "It is a change of internal priority of the incidence

motivated by a non-disconnected alarm signal" and in "extended description":

"Change the priority because the incident is sent to a manual queue.", "name

of information" "PRIO 25---20."

--"Linking directly or through inference, to a behavior or information of a natural person": "There is no direct link to customer information to the extent that they are informative signals of a technical nature". and in "des- extended encryption: panel coverage level", "name of the information: se- informative signal".

--"Linking directly or through inference, to a behavior or information of a natural person": "This log line, although it provides information about a jump alarm in the sensors, to the extent that direct information is not transferred on an attribute of the data subject nor does Securitas Direct intend to analyze a pattern of conduct or influence him in any way, the information provided by the log line analyzed should not be considered as personal data. In this sense, it would be of a description of the technical and internal process of Securitas Direct", and in "description extended": "These log lines describe the process of the system and sensors in detection of an intrusion. "Denomination of the information:-"INTRUSION VOLUMETRIC RADIO, 27 11 2015, 20:09:47

--"Linking directly or through inference, to a behavior or information of a physical person": "The signal, given its relevance, is transmitted to a machine operator machine or human to start the management process. However, it is a process internal data from which no personal data of the user can be inferred", "external description tended": "Indicative that the incident is transmitted to a human or machine operator na", "name information (...): 0".

-The only one that includes periods of days and dates indicates: -"Linking in a di- directly or through inference, to a conduct or information of a natural person": "Without detriment to the fact that as a result of any of these signals some type of action may be initiated. situation that does involve the processing of personal data, the procedures and procedures internal verification processes are essentially technical and it is not possible to infer any some personal data about them", "extended description": "They describe periods in where there is a loss of connection between the Securitas Direct servers and the device installed in the address of the interested party. In this way, the devices emit a periodic technical signal to confirm that it is indeed in connection and ready to carry out their activity. Also, the logs describe the internal and technical actions carried out as a result of this disconnection", "denoinformation mining: (...) TRANSFER".

--"Linking directly or through inference, to a behavior or information of a natural person": "There is no link with the user to the extent that

This is an internal procedure that must be followed to provide the service correct", and in "extended description": Technical information that the incident is transferred to a human operator for management.", "name: GTI: incident cancelled, client already exists in manual queue 14".

- -"Linking directly or through inference, to a behavior or information of a natural person": "Information of a procedural and internal nature of Securitas Direct", without extended description, "name of the information: GTI: incident cancelled, pending maintenance".

--"Linking directly or through inference, to a behavior or information of a natural person": "This log line, although it provides information about a jump alarm in the sensors, to the extent that direct information is not transferred on an attribute of the data subject nor does Securitas Direct intend to analyze a pattern of conduct or influence him in any way, the information provided by the log line analyzed should not be considered as personal data. In this sense, it would be of a descriptive of the technical and internal process for the disposition of the images of the detectors", and in "extended description: These log lines describe the different processes of the systems and sensors since the actual intrusion is detected: detection zone, image capture, availability of the same for the operator ador, etc.", "name: PIR Radio photo intrusion", is considered personal data is added: "NO (notwithstanding the foregoing, the captured images, in case there are have captured a subject, they would be considered personal data and should be provided to the interested party in the event that they had recruited him and not a third).

--"Linking directly or through inference, to a behavior or information of a natural person": "Information of a technical nature of Securitas Direct in relation to with the movement detections through the different sensors of the system", and in "extended description: System information in relation to a request for fotography or image", "name of the information: Informative signal". Indicates no is considered personal data, "Notwithstanding if these detections could imply the recollection of some type of information from an interested party, they could consider tion of personal data and should be provided to the interested party in the event that they they would have captured him and not a third party."

--"Linking directly or through inference, to a behavior or information of a natural person": "no information is provided in relation to any character-characteristic behavior pattern or other user information", without extended description, "name of the information: no reason."

--"Linking directly or through inference, to a behavior or information of a natural person": "information of a technical nature from Securitas Direct", without description extended mention, "name of the information: power cuts: incidence with restoration."

In table II, "information considered personal data in relation to the request for

analyzed access" (p. 31 to 48/105). In the column "Is it likely to be pro-

portioned in response to the exercise of the right of access of the interested party?, usually

figure Yes, but in some there are observations with caveats and in one figure,

NO.

The defendant informs that "certain records in the tables of this Annex ca-

They are of a specific date because they are general comments, independent of

tes of a specific line and with transversal affectation to the entire document."

-They appear without date:

-"Linking directly or through inference, to a behavior or information of

a natural person: "Of the joint information provided by: (i) alarm mode

selected by the user; (ii) date of the specific log and (iii) information derived from the

"time of (...)", the knowledge of certain behavior patterns of

a user (e.g. from a certain hour in the afternoon on weekdays the interested party

applies a (...) determined with what it is possible that you are not at home)",

"extended description: "alarm connection mode and time the alarm takes

connected in said mode", "name of the information: (...) and time of (...)."

- "Link directly or through inference, to a behavior or information of

a natural person: The highest priorities are directly related to the user

while low priorities correspond to logs of control and technical verification.

co from which user information cannot be inferred”, “extended description:

The different figures included in the column "***COLUMNA.3" of the log are priorities

assigned according to the type of signal being received. The lower the numerical value, the higher the priority.

ty (generally with the interested party's own actions such as SOS calls); to ma-

higher numerical value, lower priority (generally related to incidents of

technical character). There is an added annotation of: "Is it likely to be proportionate?"

nothing in response to the exercise of the right of access of the interested party?": "Only

Select those priorities qualified as high and connected with an action or situation.

particular decision of the interested party (e.g. priorities linked to situations of panic or distress)

rro).”

--"Linking directly or through inference, to a behavior or information of

a natural person: these denominations of the areas, insofar as they are areas of the

property of the user defined by the same and carry information about the choices of the user.

interested, would imply personal data”, “extended description: throughout the log

find denominations, decided by the interested party, to name certain areas

of the property, perimeter example, garage door, etc.”, “name of the information

mation: user defined area names on all blogs”

-Already with the log date, they appear, in all of them, that they are considered personal data, and

among others:

-"Linking directly or through inference, to a behavior or information of

a natural person: insofar as they are configurations carried out

by the interested party would imply knowledge of characteristics and preferences of the same

so they would be considered personal data", in "extended description

the device informs about different characteristics related to its configuration and pro-

programming, for example, in entry and exit times, siren volume, among others”,

“name of the information signal information”.

-"Linking directly or through inference, to a behavior or information of a natural person”: There is no direct link to information from a client

to the extent that they are informative signals of a technical nature and are not provided provides information regarding any characteristic, behavior pattern, or other information of a natural person.", "extended description: Automatically generated code automatically and randomly by the system for the security guard to deactivate the alarm”, “referred to as information mining: central high priority”. “It is likely to be proportionate Is it in response to the exercise of the right of access of the interested party?" ": No.

11/27/2015

It is unknown why it is not classified in Table I.

- "Link directly or through inference, to a behavior or information of a natural person: Direct action of an operator”. “Extended Description“: “The operator begins incident management and makes verification calls to the user and other persons indicated by the same in case of incident.” “name-information actuation Central Receiver Alarms-call to H/E”- “Is it suscapable of being provided in response to the exercise of the right of access by the interested?" "In this sense, without prejudice to the fact that it is personal data, it is of the operator and not of the interested party who exercises his right of access, since he does not It is information about said interested party.”

- "Link directly or through inference, to a behavior or information of a natural person: The actions of an operator, which includes interaction with the user or the contacts designated by the latter, involve obtaining information about about said interested parties", extended description: "Different generic actions of the Securitas Direct human operator in the event of a specific incident (e.g. authorization from speaking/listening calls to the different listed contacts; internal comments on regarding the information transmitted by contacts, etc.).” denomination of the CRA performance training” “Is it likely to be provided in response to the exercise of the right of access of the interested party? “They should only be provided as part of the right of access to the records of actions directly related with the applicant for the right and not the rest of the communications with other authorized users or contacts provided by it. Also, you should not provide the applicant with any information or analysis on the performance of the operator provider, to the extent that it is a third party other than the interested party who had exercised the right of access”

- Linking directly or through inference, to a behavior or information of a natural person: The actions of an operator, which includes interaction with the user or the contacts designated by the latter, involve obtaining information about about said interested parties.”, “extended description. The contacts that the operator of Securitas Direct tries to locate they do not answer", "name of the information “CRA-communicating performance. Is it likely to be provided as an answer to the exercise of the right of access of the interested party? However, they should only be provided as part of the right of access to the records of communications related to related to the applicant for the right and not the rest of the communications with other authorized users.

- Linking directly or through inference, to a behavior or information of a natural person”: The actions of an operator, which includes interaction with the user or the contacts designated by the latter, involve obtaining information about

about said interested parties.", name of the information, "action CRA-salta mailbox

of voice" It is likely to be provided as a response to the exercise of the right

of access of the interested party? However, they should only be provided as part of the

right of access to records of communications related to the applicant

of the right and not the rest of the communications with other authorized users."

-Linking directly or through inference, to a behavior or information of

a natural person": The actions of an operator, which includes interaction with the

tacts designated by the user, involve obtaining information about said

interested parties, denomination of the information "CRA-operator performance gets ha-

speak with contact" or "CRA action-incorrect keyword", and CRA-LO action-

CSIN-localized without keyword with "extended description: contact does not remember

the keyword to prove the identity and close the incident ""Is it susceptible to

be provided in response to the exercise of the data subject's right of access?":

"However, only the data must be provided as part of the right of access.

records of communications related to the applicant of the right and not the

other communications with other authorized users."

- Linking directly or through inference, to a behavior or information of

a natural person": These logs provide information regarding the actions

tasks of an operator, that is, the verification that he actually follows the processes

internal Securitas Direct for these purposes", "extended description: Display of

keywords by the operator in case there is a contact with the user for identification purposes.", name of the information "operator viewed codewords on demand", It is likely to be provided as a response to the exercise exercise of the right of access of the interested party? "Without prejudice to the fact that it is a data personal, should not be provided to the data subject to the extent that it affects a third person other than the exerciser of the right of access."

- Linking directly or through inference, to a behavior or information of a natural person": "The actions of an operator, which includes interaction with the user, involve obtaining information about the interested party", extended description given: "the user is contacted", name of the information: "Service Req.: ***NUMBER.1", Is it likely to be provided as a response to the exercise of the right of access of the interested party?

Linking, directly or through inference, to a behavior or information

-

tion of a natural person": Information relating to an operator of a procedural nature mental and internal Securitas Direct, "extended description" Internal registration of the operator that a specific incident is taking place", name of the information: REGISTERED ACCESS: The user ***USER.1 accessed the client file, In your case could be considered a personal data of the operator itself and, therefore, not would be capable of being transferred to the interested party exercising the right of access."

- Linking directly or through inference, to a behavior or information of a physical person": In principle, the routine tests and verifications that must be carried out The Securitas Direct technician does not provide any information about the user. unless they are specifically requested by said user, extended description given: "The technician carries out the regulatory checks to ensure the proper functioning of the systems. At the customer's request, you can modify some parameters. system itself (e.g. sound, time, sensors, etc.), name of the information

mation: Compulsory tests and verifications as part of the maintenance of the ins-

felling". Is it likely to be provided as a response to the exercise of the right?

cho of access? If the technician introduces modifications or specific configurations

in the device at the request of the user, these parameters would be considered

as personal data that must be delivered to the interested party."

-" Linking directly or through inference, to a behavior or information of

a physical person": The registration of user actions supposes the obtaining of information

personal training on it", "extended description alarm cancellation

for the user codes to be entered", "name of the information: code-

user charges", "It is likely to be provided as a response to the exercise of the

right of access of the interested party?, YES."

- "Link directly or through inference, to a behavior or information of

a natural person": The record of actions related to a real intrusion, in case

of having captured an image of the intrusion provides personal information",

extended description: log line that refers to the image captured by the

systems when detecting a real intrusion. Name of the information "VIDEO-VID"

Is it likely to be provided as a response to the exercise of the right of action?

termination of the interested party? should not be provided to the requester of the right of access information relative to the images captured to the extent that it showers information

deals with an interested party other than the exercise of the right of access"

- "Link directly or through inference, to a behavior or information of a natural person": the record of user actions supposes the obtaining of information personal training on it”, extended description: service injected event from the application by the user- remote connections and disconnections. Divermany requests made from the user's mobile terminal”, “name of the incentral formation security low priority”

- "Link directly or through inference, to a behavior or information of a natural person": the record of situations that may affect the user such as the communication of a power outage involves obtaining information staff about the same”, “extended description: in this case the client is informed by means of an email from a (...) due to a power outage of your alarm”, “ denomination of the information electric current car”.

-Linking directly or through inference, to a behavior or information of a natural person": the record of user actions supposes the obtaining of information personal training on it”, “extended description: des(...) by app client remote web”, “name of user code information”.

-Linking directly or through inference, to a behavior or information of a natural person": the record of user actions supposes the obtaining of information personal training on it”, “extended description: confirmation of (...) extotal external, “name of the central information safety priority low

In ANNEX II, entitled "GENERAL STUDY ON THE CONSIDERATION OF DATA PERSONNEL OF EACH LOG”, (p. 53 at the end) we proceed to carry out the analysis, “generally”, and “without specific application to a specific interested party”, of the consideration as personal data from the generic log lines that can normally be be used in the Securitas Direct systems during the development of its activity.

“Those log lines not derived directly from the sersecurity system defects provided by Securitas (i.e. logs with denomination

tion: FR0 to FSZ; ROF and ROI). Likewise, they have not been the object of study

The log lines that, according to the information provided by Securitas, do not

have practical application at the date of writing this report: IAC, ICA, PID,

PDD, TLL and TWC"

The table contains the identification of the logs based on three columns.

-The first column includes the "(...) of the signal", in alphabetical order, which usually includes

learn a code of three capital letters, which is "described" in the second column.

na with a general description, usually in English, some keys like FG ,SK

masking", OPDI Shutter, Sent when CP detects RX failure in FG, which they then refer to

in the third column: "extended description provided by SD"

It is observed that keys that appear in the document delivered to the claimant on

12/14/2021, in the "Signal classification" field, such as RPT, IGC do not appear in those classes.

see Annex II. In addition, there are codes such as the TAC that appears delivered to the

claimant as data and in annex II it is indicated that it is not personal data.

There are also keys (TTR or TTS) that appear NO in Is it considered personal data?

nal?, which indicates "This log line, although it conveys information about a possible sabotage,

The sensors do not provide information directly about the interested party or,

neither, on a pattern of behavior or an analysis of his personality. Therefore

to the extent that direct information about an attribute of interest is not conveyed

sado nor Securitas Direct intends to analyze or influence a pattern of conduct in

In any way, the information provided by the analyzed log line should not be con-

considered as personal data. In this sense, it is a description of the process

Securitas Direct technician and intern”

Some keys are related to “extended description provided by Securitas:

carrying out Securitas tests to verify the status of the FOG system”, or in another

“verification under the Securitas Direct action protocol of the status of the system

ma FOG”, or “information coverage level (…) of panel”.

-The fourth column is titled: "Linking directly or through inference, to

conduct or information of a physical person”, in which it is introduced in some lines

lines the reasoning on this question, and that as a consequence, gives rise to the information of the last column, called "Is it considered personal data?" with if, or

No. In the no, it can be associated with: "There is no direct link with information

of a client insofar as they are informative signals of a technical nature

and no information is provided in relation to any characteristic, pattern of con-

conduct or other information of a natural person.”

2) Summarizes its actions over time, after obtaining the aforementioned report, in order to

to assess their performance in the exercise of the claimant's right.

a) -02/26/2021, response to the burofax received on 02/9/2021, in “in which we are required to

the “logs” generated by the alarm system for the requested period. In this writing

To provide the "logs" that we consider to be personal data, as they are

registered in our systems, and due to its configuration a description is included.

tion of it in order to make them intelligible, something that exceeds what we could do.

be done. This letter was received by the claimant on 03/03/2021. See pgs. 26 to 31

of the documentation in the file. “

-18/05/2021, as a consequence of the receipt of file E/04382/2021 (transfer- of the claim in the procedure for the exercise of rights of the then: TD/ 00167/2021), "the claimant is sent again, by email, the same response provided on 02/26/2021, that is, the “logs” that have been considered to be da- personal coughs. in accordance with the report made.

-12/14/2021, it is sent to the claimant again, as a consequence of the resolution of the Appeal for Reversal No. RR/00658/2021 against TD/00167/2021, the same information mation provided in the writings dated 02/26 and 05/18/2021. "This time in a different format, per event, rather than aggregated, to make it easier to understand these. See pgs. 153 to 160 of the documentation in the file.”

“They have been sent in two different formats, grouped by event and individualized, as they are registered in the systems by event date”, “including information information that would allow the claimant to understand it”. It includes a des- description of the meaning of the event. “The records generated by the systems have been contributed as they are generated in them, and even so, efforts have been made to in- They even exceeded the obligation of my client, so that the receiver could find tend the event they reflect.”

3) “SECURITAS DIRECT in writing submitted to the Agency on 06/18/2021, pages 106 and 107 of the file (within the TD/00167/2021) showed that it generates ro logs until 8:09 p.m. on 11/27/2015, time and date on which the in- burglary of the claimant's residence and during which said alarm system was completely disabled from that date could not generate more logs.”

In relation to the internal memory of the device, the one claimed also demonstrated I state in its letter of 06/18/2021 that "after the analysis of the internal memory of the alarm installed only had a log generated for that time frame which

It was recorded in our burofax of 02/26/2021 ”.

He considers that "in December 2021 he had executed the exercise of the right of

access to data made by the claimant repeatedly”” in two formats

different, grouped by event and individualized, as recorded in the

systems by event date. A description of the significance of the event is included.

"The Agency considers in the initiation agreement that, without prejudice to having sent

4)

to the claimant the records and signals requested and generated that are data

personal, “it would be possible to have provided all the “logs” to the

Agency, down to the smallest detail and mark them as confidential in the event that they are

opposed any eventual diffusion”.

It calls into question the possibility of addressing in this way the right of access, to

not be reflected in any standard, considering it an indirect access to information through

through the AEPD, even when these are not personal data. Indicates that

has sent the claimant the personal data contained in the requested information

after its conclusion of its legal analysis report on logs, "within the period

requested”, “in two different ways”, and on three occasions.

5) Those that do not consider personal data are "logs of a technical nature, signals

information, descriptive records of internal and technical processes, configurations

of devices or statistical information, information containing technical processes

SD internals whose disclosure to third parties would imply in many cases the

communication of our know how".

"Wanting to comply with what was stated by the Agency in the written agreement

start", attached:

DOCUMENT 2, Excel table, which "contains all the records issued by the

alarm system on which the request falls "ordered chronologically", of

so that they appear sequentially, as they are produced: "In green color are data

personal according to the report.", and those of "red color, those that are not,

because they are technical and confidential, being subject to the regulations of secrets

industrial, and can be used only by the Agency".

"Of the total logs collected from the claimant's alarm system for the period

requested- 412 records- a total of 412 records have already been made available to the claimant.

273 records."

The Excel sheets provided are similar to the format provided to the claimant on

12/14/2021, and "reflect the records as they are, and appear recorded in the

systems."

Sometimes logs of the same date and time appear that are seen to be

considered personal data and another that is not, appearing with different keys of the "(...) of the

event", distinguished in red those considered not personal data, example

11/27/2016 20:09:47. There are even two logs in red, not personal data, at the same

Date and Time.

DOCUMENTS 3 and 4, Excel tables, somehow related to 2. They gather in

separately, those that are personal data logs (3), and those that are not (4), also in

the same colors as document 2. Document 3 contains, according to the

claimed, "the records issued by the alarm system on which the

petition. This document was provided to the claimant by burofax dated 12/14/2021 and reflects the records as they are, and appear registered in the systems.” Appears ordered chronologically, the first date being 11/27/2015, 8:09 p.m., and the same day there are several records, the last one at 20:17:07, and the next one goes to 12/4/2015, 11:05:04

Document 4, with the technical logs that are not considered by the defendant of personal character, begin in the record on 11/26/2015, and the following date is 11/27/2015, being the first of 9:39:43, and the last of 20:11:34. Despite the statement of the defendant that the alarm was destroyed on 11/27/2015 at 20:09, there are logs (technical only) between 11/28 and 12/4/2015, except for 11/29. Each day, four logs are reflected, with the common term “GTI MISSING TEST”, (Log that reports loss of communication with the device) up to 4, one per day. The day 12/4/2015 figure GTI: canceled incident, customer already exists in manual queue 14, without any key in description or signal classification.

It summarizes that the logs associated with the claimant's alarm system that "does not we consider data of a personal nature”, are of a technical nature, signals

information, descriptive records of internal and technical processes, configurations of devices with statistical information, information that contains processes internal Securitas Direct technicians whose disclosure to third parties would imply in many cases of communication of our "know now" with the damage that could be caused by directly and with respect to the safety of all its customers indirectly”.

6) -About the amount of the sanction of the initiation agreement:

a) Regarding 83.2.a) of the GDPR, consider that 2017 cannot be taken as temporary start date as an aggravating circumstance since the first guardianship that year was inadmissible by the Agency on the grounds that the logs were not considered data of a character staff.

“Regarding the time elapsed in connection with the damage caused and the safety of the facilities, the claimant has not gone to court, always through administrative data protection, having used the claimed the "levers laws" that agreed to their right and were offered within their reach, which cannot be penalized." A response was given to the requested access before the start of the disciplinary proceedings up to three times.

b) Regarding article 83.2.b) of the GDPR, “negligent action”, based on the fact that the claimant considered in October 2021, subjectively, that it had not yet been complied with his request, he considers that it is not an entirely true approximation, since that he had complied with the exercise of the right of access on two occasions, in February and May 2021.”

“What happened in December 2021, because this part, said without intention of offend, he no longer knew how to comply again with the exercise of law, he proceeded to submit to the claimant the same information already submitted in February and May of 2021 but with a different format (if both documents are collated, you can check that the information of both is the same). Furthermore, in none of the resolutions issued by the Agency, the possibility of contributing to it the all the logs, marking the confidential ones, "as if it has been done in this initiation agreement, without determining which article of the current regulatory framework I contemplated such a possibility”. The mere and repeated disagreement of the claimant, not must be, by itself, the cause that motivates the infringement or, failing that, the imposition of a fine"

7) Regarding the statement that there is a link between the offender's activity and the data processing within the framework of the provision of its services, considers that precisely, what is at issue in this case is whether the logs generated by the alarm are personal data or not, something, that after the report that has been provided as Document 1 allows us to differentiate that some are, that they have been delivered in various occasions to the claimant and others that are not.

8) It considers that there are proven a series of mitigating factors that would allow the application of “a degree less than that proposed in the initiation agreement”. These mitigations would be:

a) It cannot be described as not having responded to the requests for the exercise of the right as a serious infringement of article 72.1.k) of the GDPR, given that access was given in

February and May 2021, in part, but not in full, the right if it had been attended,

"It would be a mitigation to apply to the aforementioned article and consider it as a minor offense that would fit into article 74.c of the LOPDGDD.”, which indicates:

"The remaining infractions of a legal nature are considered minor and will prescribe after a year.
merely formal of the articles mentioned in sections 4 and 5 of article 83 of Regulation (EU) 2016/679 and, in particular, the following:

c) Failure to respond to requests to exercise the rights established in the Articles 15 to 22 of Regulation (EU) 2016/679, unless it is applicable provided in article 72.1.k) of this organic law.”

-There is due diligence, "for the sole purpose of complying with the claimant's request and of the scope of the right of access to your personal data, making an effort, including economic, was placed in the hands of a third party independent of

recognized prestige, for the purpose of disaggregating, among all its logs, which are

those considered as personal data (according to the definition of "data of

personal character") and which are not, and which are trade secrets"

-There is good faith, as demonstrated by the fact that "the right has been complied with

up to three times", "once he was clear about the criteria that logs are data

personal and which are not”, always giving the same information. Depending on the criteria

of the AEPD, based on the initial agreement, all the logs have been provided.

-Considers that the action of the claimant expressing his dissatisfaction "with what

subjectively, it considers what the logs are and how they should be represented

on paper, it cannot be an additional condition for him to propose to impose

a fine that they understand to be disproportionate, but the opposite, should be grounds for

that the penalty is less than the proposal.”

Request that the exercise of the right be considered fulfilled with all the logs now

contributed.

SEVENTH: On 11/23/2022, it was agreed to start a test practice period.

1-The claim filed by the

claimant and its documentation, the documents obtained and generated during the

phase of admission to processing of the claim, and the report of previous actions of

investigation that are part of procedure TD/00167/2021.

Likewise, it is considered reproduced for evidentiary purposes, the allegations to the

initiation of the referenced disciplinary procedure, presented by the defendant, and the

accompanying documentation.

2-Because they are related to the original petition, they are incorporated as evidence into the

procedure:

a) The documentation provided by the claimant and that obtained and collected from the claimed regarding the protection of rights 1564/2016, resolved on 09/08/2016, as well as documentation of both parties produced in its processing.

b) The documentation provided by the claimant and that obtained and collected from the claimed regarding the protection of rights 1593/2017, as well as documentation of both parties produced in the appeal for reversal resolved on 01/2/2018, RR/779/2017, and the documents that are part of said files.

c) The documentation provided by the claimant and that obtained and collected from the claimed regarding the protection of rights resolved by Agency TD/00167/2021, the procedures related to it, including the transfer of the same to the defendant E/4382/2021, and the admission for processing and management and processing thereof, as well as the subsequent reversal appeal resolved RR 658/2021 of 10/27/2021.

d) The Judgment of the National Court (AN), Chamber of Administrative Litigation first section, of 07/23/2019, resource 146/2018, and by relation, the order of the TS room of Administrative Litigation first section, of 05/29/2020 number of procedure 378/2020 for admission to processing of the appeal of the claimed, from which he later withdrew, appearing as such, in the order of the TS, appeal 378/2020 of 09/15/2020 in which it is indicated that the representative of Securitas "presented a brief on 07/24/2020, withdrawing from the appeal prepared", declaring "terminated the appeal for withdrawal", and communicated to the AEPD in writing of the Lawyer of the Admin. of Justice of 10/29/2020, appearing as an associated object of the file: PS 2181 22 san and ts.

3. The defendant is requested to provide or report within fifteen days:

3.1-Provide a copy of the terms contained in the exercise of the right of access

Formulated by the claimant on 02/02/2021.

Response received on 12/30/2022.

In the first place, it stresses that the procedure followed is for infringement of the

Article 58.2.c) of the GDPR:

"order the person in charge or person in charge of the treatment to attend to the requests for

exercise of the rights of the interested party under this Regulation".

For this, it considers relevant the distinction between the logs that have the condition of

personal data or those that refer to "aspects simply related to the

operation of commercialized alarm systems, the disclosure of which could

generate a violation of their right to trade secret, and the risk of

its future operation, by informing third parties unrelated to the

organization".

He believes that some of the questions that are raised in tests by the instructor,

"They are not related to the object of the procedure, but rather to the appropriate

operation of the contracted alarm system". The information you will provide

will be circumscribed "to the object of the procedure", on whether it gave "adequate compliance to

what was agreed by the AEPD", as well as "if the information that was not provided to the claimant,

in application of what has already been invoked in the allegations, they did or did not contain personal data

of that, without understanding that it is appropriate to provide information related to the behavior in relation to the events that occurred at the claimant's home."

Provides burofax of the claimant on the exercise of law signed on 02/02/2021, with shipping 02/9/2021, handwritten: received 02/10/2021.

The brief is based on the fact that "on December 4, 2015, the house suffered a assault and robbery without the indicated alarm system being activated, which detected, issued and received the proper alarm signal, being seriously damaged the switchboard and resulting in the first news that Securitas Direct Spain had was the Call from my represented, reporting on it. The alarm system came suffering certain incidents with certain connectivity problems", to pass to assess the demandability of the claimant by Securitas for the replacement costs of the switchboard, after the incident, the suspension of the service from 12/23/2016, apparently by cut due to non-payment of replacement costs, indicating the holders who gave for terminated the contract and in turn requires a series of refunds of amounts in various concepts.

Immediately afterwards, it reiterates the request for the information on servers regarding the records and signals sent by the alarm equipment between 11/26 and 12/18/2015. He mentions the sentence of the AN, its firmness and requires his compliance.

3.2-Copy of the contract signed with the claimant in which the conditions appear general and specific information on the service and the exercise of rights, including clause 14 of the privacy policy to which it alludes in its exercise of rights from 04/07/2017.

Copy of the instructions delivered to the user, in writing, of the operation of the service, informing you of the technical and functional characteristics of the system and the responsibilities that come with joining it.

It is provided, as DOCUMENT NUMBER 3 contract number *** NUMBER.2

entered into on 07/30/2014 with the claimant (hereinafter, the “Agreement”), including, in

pages 9 and 10 of the document, clause 14, referring to data protection

personal.

From the "security service" contract, it is worth mentioning:

Particular conditions:

-Personal data is collected: e-mail, name, surname, address and telephone.

-The service includes the installation, maintenance and operation of

alarms.

General conditions

-"2. description and scope of the services object of the contract, A) service of

installation and maintenance”, states that the installation will include the elements and

components contemplated in the particular conditions of this contract and

Securitas Direct will provide a basic maintenance service that includes for the

client: remote verification services of the operation of all

components (technical check according to current regulations).

It also refers to the definition and distinction of fault, "the damage that prevents the

proper functioning of a security system to fulfill the purpose for which it is

is intended" and "technical problem" "that incident that implies the necessary

intervention by SECURITAS DIRECT for verification, whether or not in person, and that,

In no case prevent the full operation of the security system of the vehicle.

CUSTOMER."

Point B) refers to the connection service to the alarm receiving center.

-in 6: "customer obligations", it is established among others:

a) "You must, in any case, connect the alarm system every time you intend to avoid the access of unauthorized persons to the place and, especially, each time the place left abandoned and unguarded. Accreditation of the alarm connection corresponds, in any case, to the CLIENT. Therefore, the contracting of the service of all the controlled codes will be a requirement to reliably prove the alarm connection status. If the CLIENT has not contracted the service that allows you to prove that the alarm is connected, it corresponds to him to prove the connection because the connection is an act that derives from the actions of the contracting party the service and not SECURITAS DIRECT."

o) Notify at all times possible changes in contact persons or telephone numbers in case it is necessary to locate him."

"10. RIGHTS OVER THE INSTALLATION Due to the rapid evolution technology makes control and communication systems obsolete, SECURITAS DIRECT will retain ownership of the installed security system for be able to update the software and its components, for the sole purpose of providing the most advanced security services.

- 14. PRIVACY POLICY

A) INFORMATION REGARDING CUSTOMER DATA PROTECTION: The personal data provided by the CLIENT to SECURITAS DIRECT, as well as any other data that could be provided throughout the contractual relationship, will be included in a file, whose responsibility is SECURITAS DIRECT ESPAÑA, SAU…, sole recipient of the data, with the main purpose of carrying out the relationship contractual, own management of the activity, maintenance, development and control of the contractual relationship. "

"C) TREATMENT OF IMAGES AND/OR SOUNDS OBTAINED THROUGH THE SECURITY SYSTEM WHEN THE EQUIPMENT INCORPORATES SYSTEMS PHOTODETECTION. - When verifying an alarm jump by SECURITAS DIRECT

“SECURITAS DIRECT through its Alarm Receiving Center will capture and record images and/or sounds through the security devices installed in the places subject to protection of the CLIENT, in accordance with article 48 of the Private Security Regulations, that is, verifying through all means technicians within their reach the alarms received and once said verification is exhausted if If appropriate, it will transmit said images and/or sounds obtained as a result of the alarm jump treated to the competent police or judicial authority.

SECURITAS DIRECT acquires the status of Responsible for the management file of video surveillance systems with access to the CLIENT's images, due to their natural person and that the security system with access to images is made at your private home. It will not be considered illegitimate interference in the right to honor, to personal privacy and to one's own image, recruitment, reproduction and processing of images and sounds due to a jump in alarm generated by the image protection element installed and treated at through the SECURITAS DIRECT Alarm Receiving Center.

The CLIENT may only have access to information on any incident or recording made due to an alarm jump, sending a written request to through the means that allow it, indicated in clause 20 of the general conditions, in which the identity of the contract holder must be stated

accompanying a photocopy of your DNI, CIF, NIE or valid passport, as well as the date,

time and place where the recording presumably took place. SECURITAS DIRECT,

will guard the recordings obtained as a result of alarm jumps

generated by the security system installed, and will comply with its obligations of

conservation, uselessness and destruction.”

The aforementioned contract includes in its Annex I, "the installation project", with the

characteristics of the study of location and risks, with the proposal of the design of

security and with the elements configured in the installation plan, as well as the

elements and risk areas protected through verification of alarm signals

by audio, image-video, and face-to-face.

Annex II refers to the: "ACTION PLAN", which includes, among others:

-"contact list", four people identified by first and last name, ordered

by increasing number, all with “keys”. The first, the claimant, as a "client", the

person “who signs the contract, owner of the alarm system” associated with two

phones. The other three: "relationship with the subscriber": "relatives" with a telephone.

The four people are listed in the “standard action plan” in the chart, ordered

as "contact" from 1, the claimant, to 4.

-the password or "master" of the client, the duress password and the SECURITAS password.

 Within the Action Plan, the "CONDITIONS OF THE SERVICE OF

OPERATION OF THE ALARM RECEIVER CENTER" highlighting among others:

-"CLIENT: Natural/legal person who signs the CONTRACT, who is the owner of the alarm system described in the aforementioned CONTRACT and that is the holder of the word master key. The CLIENT may in any case have the status of user "

"USER: Natural person to whom the CLIENT authorizes access to the property and the use of the alarm system, making available the means of connection and/or disconnection from it.

"CONTACT PERSONS: Natural person who may or may not coincide with the CLIENT of the contract and who owns the master keyword."

2. KEYWORD It constitutes a necessary data for the provision of the service hired. Its holder is obliged to maintain its confidentiality, should not transmit it to third parties.

Keyword Types:

- SECURITAS code: Identifies SECURITAS DIRECT and must be provided by the same in any telephone communication with any of the persons described in section 1 of this document.
- CLIENT MASTER Password: Identifies the CLIENT and the main contacts. It must be provided by them when they contact SECURITAS DIRECT by phone. Allows and gives access to all kinds of procedures and modifications, whether administrative (contract, action plan, etc.), or operational (verification of alarm jumps).
- COACTION code: In the verification call before an alarm jump, you must provided to SECURITAS DIRECT, by whoever is in the property before a situation of real danger to their physical and/or patrimonial integrity

3. VERIFICATION PROCEDURE BEFORE ALARM TRIPS

The SECURITAS DIRECT Alarm Center will execute the pertinent process of verification of alarm jumps registered by the installed security system, through the means at its disposal contracted or arranged by the CLIENT, such such as, speaking, listening, image and/or call to the fixed telephone of the property, calling the contact telephone numbers provided by the CLIENT in this document and, in its case, sending the Go Service accompaniment to the Police or the Go Service to Full Service verification, in the event that the CLIENT had contracted the latter service.

SECURITAS DIRECT will issue the corresponding notice to the Security Forces and Bodies Security (hereinafter, "F.C.S.") only in the event that reality is proven of the event generating the alarm jump, once the verification has been carried out valid, through existing means, in accordance with current regulations in private security matter.

For the purposes of initiating the action protocol, the alarm signals are considered to be received at the Alarm Receiving Center from the capture of the intrusion detection elements, the SOS button, the anti-robbery button, and the coercion.

-In the contract there is a section that includes the protocol in cases of jumps in alarm, "from pressing the SOS button, anti-robbery button, code of duress and when the duress keyword is provided.", in case of “without user disconnection”: verifying “by accessing the speech-listening module of the system and/or call to the fixed telephone number of the property, as long as this is available last. If through these means:

- An answer is obtained: the person will be identified with the keyword teacher or contact If the keyword is correct, the user will be provided with the precise technical instructions for you to disconnect the system.

- If the keyword is not correct or no response is obtained: SECURITAS DIRECT will proceed to comply with the verification procedures provided in the current Private Security regulations as well as to use the media complementary verification procedures such as proceeding to the verification call to the MAIN and/or OPERATIONAL CONTACTS established, and/or the Warden of Security and/or F.C.S. if it were a confirmed real alarm. In any case, the The decision to issue the notice will correspond exclusively to SECURITAS DIRECT.

In the event that "user disconnection" occurs, it is the case in which the alarm, and in less than 20 seconds (from the alarm jump), it receives disconnection signal in the CRA. In this case, "an automatic locution recorded through the speech listening module of the system, in which will inform the client of the signal received as well as of the execution of the disconnection by the user or authorized person and the cancellation of the incident"

"In the event that the disconnection signal is received in a time greater than the indicated in the previous paragraph, SECURITAS DIRECT will proceed to verify the jump of alarm by accessing the system's speech-listening module and/or calling the Landline telephone of the property, provided that it is available, to carry out the verifications that it deems appropriate according to its diligence as a Company of Security and that are adjusted to the applicable Private Security regulations."

In document ANNEX III "certificate of installation and connection", it is indicated that "the security elements and devices installed to the client correspond to the security level 2, established in article 2 of order INT/316/11 of 1/02 and have the corresponding approval according to the characteristics established in UNE-EN 50130, 50131, 50132, 50133, 50136 and in the UNE Standard

CLC/TS 50398

- In a table, the type of device of the elements that make up the system appears

installed.

As DOCUMENT NUMBER 4, it provides the user manual of the

□

alarm (hereinafter, the "Manual") in its existing version at the time of the

contract with the claimant. Highlights of it:

-Control panel with GPRS transmission: GPRS communications (...), SMS, card

Securitas Direct SIM included. Supports image transmission. Talk/listen loud

sensitivity. The only one with a personal portable intercom to ask for help.

SOS button. Indoor siren. Supports up to 32 home automation control user interfaces

-Key reader/smart keys: allows you to easily activate and deactivate your alarm

without having to memorize complicated codes. Different modes can be activated: day,

perimeter…

-Motion detector with color camera and flash from our central station

we can see what happens in your home or business in case of alarm

take sequences of images built-in flash for night vision and deterrence

-Communications: "supervision of communications through a periodic test."

-For activation, it has various modes, how fully activated when leaving your home

so that all the detection zones of the security system are protected.

security, or partial modes: that can be activated day mode or activated mode

night or perimeter mode activated.

In description and use of the control panel with keyboard, the different

functions of the buttons listed, from the SOS function, in case of emergency that

can be sent to Securitas Direct with a light indicator indicating that it has been

correctly received the coverage light signal from the control panel, “(...)”,

“hands-free” function to receive incoming calls and to answer,

calls to 112, and another series of functions.

3.3-Description of the operation of the contracted alarm system that was installed in

the claimant's property, composition of elements (switchboard of the

alarm located in the home, its components, control panel, sensors or

alarm detectors included in the system, alarm kit or other

system accessories and connection to the Alarm Receiving Center).

They are also asked to report the system or communication channel used by the

device installed in the claimant's home.

Point out that the manual describes on pages two and three the basic elements of

alarm system

The contract also included in terms of additional elements contracted:

A remote control, to connect-disconnect the alarm.

An external siren flash, which is located inside the installation and sounds when,

for example, the alarm is activated.

Two magnetic detectors, two seismic detectors (although the contract includes Separately, they are the same devices, known as “shocksensors”, that detect opening, closing and vibration, do not collect images.”)

An element of verification by audio speaks listens, "(It is located inside the control panel and is to perform audio and listening checks in case of jump alarm, it is also used to talk to the customer through the switchboard).”

Three verification elements by video sensor photodetector image, (Detectors with camera that react to temperature changes detected by movement, in such a way that, if they detect movement while connected, they trigger the alarm and collect images.)

An external perimeter detector with image (Same description as the photodetectors but from outside)

A smart key reader (tag reader) which is the device used to arm/disarm the alarm. Which is related to 6 tags (intelligent keys that are are used to disconnect the alarm by passing them in front of the key reader smart.

“The only modification with respect to the initial state was the change of the two magnetic/seismic by three volumetric devices, which are cameraless detectors that react to changes in temperature detected by movement, so that if they detect movement while connected, they trigger the alarm”. It indicates then that after discharge from service, at the time of the intrusion there were three photodetectors, and three volumetric, in addition to the rest of the elements already mentioned.

Refers to the information included in the manual to complete the operation of the system.

"Regarding the connection system with the Alarm Receiving Center (hereinafter, “CRA”), this is carried out by means of a SIM card integrated into the control panel.

control."

3.4-a) Way in which the logs of the operation of the system are generated and stored alarm system. If in addition to the operation or generation by the machine, is Can Securitas operators create logs? Under what circumstances?

It states that "the system generates and stores records derived from:

-Customer interactions with the alarm system, for example: connection, disconnection.

-Internal verifications of the system: example coverage (...), and

-Activities of the alarm system in the performance of its function, for example jump alarm.”

"Regarding the possible generation of new logs by SECURITAS operators DIRECT, it is necessary to indicate that the catalog of logs that can be generated by the interaction of the installed system and the CRA is closed, that is, it is not possible to creation of new logs other than those that the system allows to generate. For other part, obviously, some of these previously configured logs will be generated as a consequence of the interaction of the system with an activity carried out by an operator or user authorized by SECURITAS DIRECT, as well as by the owner of the system or the persons authorized by it. However, as has been indicated, they would be found in the catalog of those that can be generated in the system and would not present any type of novelty with respect to the existing ones, be it impossible."

b) Report if the alarm system control unit itself is capable of storing

records or only originates and sends signals, and which signals or records originate and which

it would be fate.

He replied that: "The switchboard (control panel) of the alarm system is capable of

store records, in fact, holds ***NUMBER.3 events which are

deleting cyclically, depending on the records that are generated and

recording continuously. As new records are generated and recorded,

they delete the oldest ones maintaining a temporary order of recording and deletion

always within the ***NUMBER.3 records that it can hold."

Within these recorded events, a distinction must be made between:

(i) those that generate a log, a copy of which has been provided in the

Document No. 2 of those provided together with the pleadings to the Agreement of

Start (they collect mixed technical logs together with those considered data logs of

personal character, in sequential order of date and time, with keys of: "classification

signal", key that is specified in ANNEX II of allegations to the initiation agreement together

whether or not it is considered personal data and why), the description, the most

wide (called in column "(...)"), comment, event, event extension,

priority, zone.

(ii) and other merely technical events related to the interconnection

produced for the submission of the logs to the CRA of SECURITAS DIRECT (e.g. channel

by which the log is sent, successful connection, acknowledgment, etc.). Since the

mentioned in point ii only refer to the referral and not to any type of

specific action, not generating a log, would not be part of what was requested by the

claimant.

"The destination of these records is the CRA, although the information mentioned in the

point (ii) as well as the logs that do not reflect a relevant event related to the alarm operation are not communicated and remain in the internal memory of the switchboard and are only accessible by SECURITAS DIRECT personnel in case of an event occurs that requires forensic analysis. Throughout case, the logs that remained in the internal memory of the switchboard disabled by the action occurred on November 27, 2015 have been incorporated into the information provided in the aforementioned Document No. 2 of the pleadings to the Agreement of Start."

c) When talking about the internal memory of the device, where is that internal memory located? What events does it record, differences with the signals that it can send to the control center? alarms the control panel? .

It responds that it is housed in the motherboard of the switchboard-control panel-.

As for the events it reflects, you have already detailed them.

d)

Inform if it is possible and under what circumstances, activate or deactivate the alarm from the CRA, and if the operation can be recorded in logs and if, in this case, it has been any event of this type occurred in the requested access period.

Answer that "From the CRA, operators have the ability to activate or deactivate the alarm only at the customer's request, within the framework of an interaction phone with him. This petition is duly registered, through its corresponding log."

"In the case analyzed in this file, said functionality was used within the requested period, and proof of this are the records detailed below.

below, which are part of the information sent to the Agency:

- (...):

o 12/18/2015 at 20:08:57 - Order sent (...) Total per user: B.B.B.. o

12/18/2015 at 20:09:08 - (...) external Total.

o 12/18/2015 at 20:19:59 - Order sent (...) Total per user: B.B.B.. o

12/18/2015 at 20:19:59 - (...) external Total.

Or 12/18/2015 at 20:20:07 - Order sent (...) Perimeter by user: B.B.B..

o 12/18/2015 at 20:20:19 - (...) external Perimeter

- (...):

o 12/18/2015 at 20:18:56 - Order sent Disarm by user: B.B.B..

o 12/18/2015 at 20:19:11 - De(...) external: ***NUMBER.4.

3.5-Verification mode/s of the applicable alarm/s in this case, and which logs are

generate and indicate those that with this description appear in the period requested by the

claimant.

It responds that "the logs that are generated to verify the operation of the

alarm can be classified as follows:

those that are generated as a consequence of an interaction of the holder of the

(Yo)

contract or an authorized by the same with the alarm system;

(Yo)

those derived from a human interaction produced from the CRA; and

those that are generated automatically, without human intervention of any

(ii)

guy.

In this sense, and taking into account that only the logs listed in the

points (i) and (ii) imply a processing of personal data, and of these only the

listed in point (i) involves the processing of the Claimant's data or the

persons authorized by it, in Document No. 1 provided by the defendant

along with his pleadings, it was clarified that the right of access by the

interested in their own data, only affected the contents in the aforementioned

point (i) and not to those listed in points (ii) and (iii), which do not include data

Claimant's personal

Specifically, and with regard to all the logs provided to the Agency, they would fit

In what is described in this answer, the following logs that represent verifications of

alarm:

- Logs from 11/27/2015 from 20:09:47 to 20:17:07,

moment in which an action plan is contacted.

- Logs from 12/06/2015 from 01:15:04 to 01:17:40.

3.6-a) Report on the aspects of configuration operation and types of

configuration of the device in the security system contracted by the claimant,

and by the different types of users that were contemplated and had access in the

device settings, if any. The way in which they are identified in the logs

the various actions of potential users in their various roles that may

assume: holder, authorized, contacts in the different elements of the system. In one

of the log names appears "user ***USER.1 accessed the client's file",

who is this user, given that in other cases they refer to the staff of the entity as “technician”, “operator”.

a) Regarding the term used in logs, "designated contact", description of who

they refer to, and their relationship, where appropriate, with those authorized to access the system, and in

In this case, if the designated contact is only the holder of the alarm contract? Relationship

of actions carried out by the owner or authorized persons regarding situations

techniques in which the system can be found, (...)/(...), and if they can be

identifiable such actions relating them to the person who interacts.

b)

Report the number of authorized Users in the contracted alarm system

per claimant, number of designated contacts, and if only the designated contact was the

holder of the contract, roles that differentiate in their actions and their limits to the user

authorized in front of the designated contact. For what type of actions each one? and

What type of actions can only be carried out by the holder?

c) Document in which the holder of the service has given the data of the users

authorized, designated contacts.

He answers that "to clarify the way of interaction of the alarm systems with the

CRA, is answered jointly. The authorized contacts are understood to be, for the

owner who contracted the system, the claimant, while the users with access to the

system would correspond to SD staff.

Authorized or designated contacts may interact, in any case or under

certain circumstances with the CRA, making a communication to it in which modification of certain characteristics of the action plan may be requested

established in the contract (e.g. delay time in the activation/deactivation of the

system, update of contact telephone numbers, etc.). In any case, that

interaction must be preceded by the keyword also established in the contract.

Likewise, the authorized contacts, in their order, will be the recipients of the

calls that SECURITAS DIRECT can make in the event of any kind of

impact on the operation of the system. In this specific case, how can

verified, the Claimant designated four authorized contacts in the Contract,

also establishing their order in the event that it was

interaction with them is necessary (see the last two tables on page 16

of the contract). Together with the authorized contacts and the contract holder, the other

natural persons operating in the system are the users, identified as the

SECURITAS DIRECT agents who can receive a specific incident

as a consequence of an interaction with the owner or those designated contacts and

where appropriate, they carry out the operations requested by them. This would give rise to the

generation of the consequent log that in the valuation attached to the document of

allegations to the Initiation Agreement were considered as personal data of the

Claimant, when proceeding from an action urged by him or his authorized.

So that authorized users of SECURITAS DIRECT are not

directly identifiable or accessible by third parties, each of them has

with a unique name or "registration" made up of alphanumeric characters

that exclusively allows its internal identification by the company. such is the code

"***USER.1" that appears in one of the logs and about the one that has been raised by the

AEPD the question of users. In this case, the registration of the interested party is recorded and not

its generic name given that the access occurred as a consequence of the

interaction carried out by the contract holder, thus guaranteeing traceability of what was requested and the determination by SECURITAS DIRECT of who attended said application.

Finally, within the users of the system, reference should be made to the remaining technicians or operators, (...). In this case, the log generated by your activity does not generate a license plate, as the aforementioned guarantee of traceability is not required.

For the purposes of the logs provided in this case, those that generate an interaction between the owner or a contact designated by the latter and SECURITAS DIRECT are the between 12/05/2015 at 14:19:04 and 14:45:45, where ***USER.1 access the customer file to manage and agree on maintenance with the customer associated with the event that occurred on 11/26/2015.

Subsequently, also at 18:38:10 on 12/05/2015, the log shows the registration ***MATRICULA.1, which is the technician who physically travels to the

address of the claimant to carry out the corresponding maintenance, and connects to the system to do it.

Finally, on 12/18/2015 at 20:08:18 the SECURITAS employee logged in DIRECT B.B.B., as a result of a customer call to SECURITAS DIRECT where it consults the connection status of the alarm at that moment. For For this, the employee must access through an internal tool, which requires the logged in from your professional email and password, through which you You can check the connection status of the system and interact with the system under what the client requests. Although this interaction is recorded in the logs, the how it should be executed is implying that in registration instead of registration

the email appears (without @securitasdirect.es). In this case, the claimant

contacted the SECURITAS DIRECT operator that is identified in these

logs and that at the moment of initiating the connection it had to be previously identified

before the Claimant, therefore the latter already had the identifying information of this

used at the time the connection was made."

3.7 a) Operation of the programming of the device when entering the home with the

security system active, to deactivate, or vice versa, to leave it configured

when the house is abandoned, also considering that there may be different

users, and how it has to operate when accessed by another user other than the one that left

programmed to output the alarm.

He replied that "the Manual incorporates the activation and deactivation procedure

of the alarm system as a consequence of the interaction of a user, not being

These effects require that activation and deactivation be carried out by a

same user."

a) Indicate if the contracted service included the control of the application with a device or

mobile telephone terminal and how it interacted with the logs stored in the

server in the requested period.

It indicates that "the contracted system allowed its activation and deactivation from the

application (hereinafter, the "App") that the user could install on his device

mobile (this application exists in iOS and Android versions). Taking into account what

above, when there is an interaction between the owner or an authorized contact that

involves the connection or disconnection of the alarm system, said incident is recorded

in the internal memory of the device, although it is only transmitted to the CRA in case of

that the action responds to the existence of a security incident. In that

of course, that is, when a security incident occurs (e.g. disconnection as a consequence of an alarm jump) and later the

system, the log is registered in the CRA identifying the user (key, command or

code) that performed the action. Similarly, if the disconnection or connection is

performed from the App, the log is transmitted to the CRA, reflecting that a

action through an Iphone or Android device, but the number of

phone from which this action is performed.

In the present case these records would be the following:

- 12/06/2015 at 1:15:27 – Disconnection. KF 00 - User: 07 Disconnection by jump of

alarm at 1:15:04 (...). This log records a deactivation of the alarm system

by means of a remote control following an alarm jump.

.Regarding logs associated with interactions with the alarm system through the

APP installed on the claimant's mobile", refers to requests from IPhones from different

type: status request, of (...), of image on various dates from 12/06/2015.

In any case, the internal memory of the control unit (Control Panel) to which it has been able to

access my client, that is, the one initially installed and destroyed in the facts

occurred on 11/27/2015, does not incorporate, within the time period with respect to the

that the right of access was exercised, no log referred to (...) or from (...) of the system

alarm, this being, and no other, the reason why the information provided to the

Claimant does not incorporate any record of this nature in relation to the

disabled device. Regarding the logs that appear in the internal memory of the

installed on December 5, 2015, as will be analyzed when responding to the question formulated in point 4.14 of the letter of that AEPD”, (3.14 of this proposal) "my principal was not able at any time to access the information, so that it was not possible for him to provide it to the interested party.”

3.8-a) If in accordance with the specific regulations of the sector of the operation of alarms, periodic reviews are carried out, what would these be, and if they are done appear in the logs, determining which are the specific logs that respond to such reviews. If the so-called record of incidents, which is discussed in the OM 316/2011 of 1/02 on the operation of alarm systems saves any relation to the logs generated by the system.

It responds that: "periodic reviews are provided for in article 43 of the RD 2364/1994 approving the Private Security Regulations and article 5 of Order INT/316/2011. These reviews would include at least the obligation to carry out only one face-to-face annual review. The SECURITAS DIRECT CRA has ability to perform these checks remotely, typically every three months. In addition, it indicates that daily tests of communication and correct Transmission of the alarm system with the CRA automatically.“

Examples of the aforementioned verifications are attached:

```
12/06/2015 18:45:42 Panel use: Tot 00, Parc 00, Per 00, Anx 00
12/05/2015 18:38:10 INSTALLATION IN TESTS
12/05/2015 18:38:10 INSTALLATION UNDER TESTS FOR MAINTENANCE -
***NUMBER.1 BY TECHN
05/12/2015 18:38:10 000:08:00 ALL ZONES
12/05/2015 18:38:10 TECHNICIAN: ***REGISTRATION.1-C.C.C.
```

"On-site reviews are recorded in the log of the management system of CRA alarms, since the technician must check a series of system parameters and carrying out the various functional checks.

Likewise, as contemplated in the regulations, if revisions were made

remote, these would be reflected in the event memory of the alarm system

(art 5.2 OM and annex III quarterly face-to-face maintenance with a possible alternative to

automated self-test and bidirectional."

b) Difference between inspections and maintenance operations of the installation

in operational state, where the latter are regulated, and through which modality they are

carry out these maintenance operations.

He indicated that "The review is a mandatory, preventive and periodic task described in the

aforementioned Private Security Regulation and Ministerial Order 316/2011, and the

Maintenance is a corrective task aimed at solving specific incidents

that do not allow the correct functioning of the alarm system, and that have as

purpose of correcting these incidents. The review is carried out, as

has been revealed in section a), while maintenance will depend

of the need and nature of the incidence, and can be carried out in a

face-to-face or remote.

3.9- If there is any relationship between the revision record books, revision record books,

alarms, incident record, OM 316/2011 of 1/02 of operation of the

alarm systems, and the logs generated by the device installed in the residence of the

claimant, if data from the logs are transferred to said books, and their relationship with the

consideration of personal data of the owner.

He replied that "Security companies, depending on the activity for which they are

are authorized by the Ministry of the Interior, are obliged to carry

certain books. In the case of SECURITAS DIRECT, you must bring the following

Books, the models of which have been officially approved by the Ministry of the Interior:

• Alarm Record Book. Completed and custody by SECURITAS

DIRECT It is intended to record the confirmed alarm messages that are

notify the Security Forces and Bodies. "In the present case, there was no

no confirmed alarm, so they would not be included in this book"" Provides

printing of part of the book in which there is no inscription.

• Company Review Record Book. Completed and guarded by Securitas

Direct, is intended to record all periodic face-to-face reviews

that are made to the alarm systems of its operational clients.

• Record Book of Communications with the Security Forces and Corps, whose

object is the record of the collaborations and assistance that are carried out during the year

with the Security Forces and Bodies.

"In none of the aforementioned books are logs or signals of the

alarm systems as recorded by the system itself, but rather the

information of that event communicated to the Security Forces and Corps

providing the data requested in the book".

3.10-To verify the way in which the raw record or log appears in the system, it is necessary to

requests that they provide a copy of the raw log:

From 12/15/2015, 4:50:24-Informative sign- which was the first to appear in to)

the right of access delivered to the claimant in his brief of 02/23/2021.

One of the logs of 11/27/2015, which appear grouped in "CRA Action",

to)

and in "extended description" there is "different generic actions of the operator

human…"

Indicates that all the logs generated in the system appear collected in its

completeness in the document provided as document two, together with the brief of

allegations to the initiation agreement.

They provide document 5 with the extract of the specific logs requested

The logs of 11/27 occupy 8 lines, central alarm receiving action.

b) Indicate how the information referred to in "extended log description" comes out before

the elaboration, or where one goes so that in some cases it is so generic or

description open. If these generic descriptions cannot be detailed

further.

He replied that "As can be verified in the information contained in the

previous answer, the “extended description of the log”, which was incorporated in the first

of the responses given to the Claimant by my client, is not contained in the logs

generated by the system, which were reproduced as they are shown in the second

of the answers. This description was introduced in the first reply to the

Claimant with the sole and exclusive purpose of clarifying the scope and meaning of

the same. In this sense, SECURITAS DIRECT considered that the information

provided to the Claimant in the rough (document number 2 of those provided together with the

allegations to the Commencement Agreement) and without a minimal description of the meaning of the

logs may be of no use to the Claimant.”

3.11-In their allegations, they indicated that:

"... the records considered as personal data have been provided in three occasions and in two different formats and including complementary information that enable the claimant to understand it. It should be remembered that the records generated by the systems of my represented have been provided as indicated generated in them, and even so efforts have been made that even exceeded the obligation of my represented, so that the recipient could understand the event that reflect”.

It is requested that they provide or inform about the complementary information that It helps to understand it and where it comes from.

It responds that "the supplementary information referred to in this question is the one referred to the “extended log description”, already mentioned in the previous section that my client incorporated into the responses provided to the interested party at the time of responding on all occasions together with each of the logs, trying to expose, even through a brief description, the actions to which each of them responded. In this sense, my client did all the efforts reasonably required to address as clearly as possible what requested by the Claimant, not limiting himself to providing the logs in the format in which they were generated in the SECURITAS DIRECT systems, but by briefly clarifying the scope of each of the Code lines provided.”

3.12 Regarding the "active interactions of the user himself with the systems in physical or through the mobile application.", "passive interactions of the user or of third parties that can provide information with their way of acting", point out examples, and if in all cases they could be personal data or not, and logs that can be found within these categories.

He responded that "The user's own active interactions with the system remain reflected in the corresponding log. In particular, reference should be made to the connections and disconnections of the alarm system, which are only registered in in case of having produced a previous alarm trip, as indicated in the response to the question raised in point 4.4 of the letter of that AEPD", (in this proposal 3.4).

Along with these physical interactions, the client may have other complementary or extras like e.g. press the "112" button that generates a direct call through from the switchboard to 112. Also, as a physical interaction, you can press the "SOS" from the switchboard and from the key reader (tag reader). Similarly, you can click a "duress code" through the numbers indicated on the switchboard or you can intentionally generate a tamper/sabotage or tamper signal, consistent to remove a device for a certain reason (e.g. because the house) or without it (e.g. because you hit it accidentally).

Finally, through the mobile application, connections can be made and alarm disconnections, query system status, review invoices or perform a request for images.

Examples related to physical interactions of the system are defined in the column "***COLUMN.2 (...)".

Regarding the "passive interactions", they do not imply the performance of an activity of the owner or his contacts, but rather contain information that, in the event of be analyzed, something that SECURITAS DIRECT does not carry out, could reveal habits behavior of those (e.g. reiteration of periods in which the system is (...), which would denote absence of the dwelling object of the security system), for which reason

considered personal data and were provided to the Claimant. Consequently,

this information is not derived from a specific log but from a more detailed analysis

of the logs that, as indicated, is not carried out by my represented.”

3.13- They stated that "we inform you that (...) the Securitas alarm systems

Direct register and store the information coming from the events with origin

technician and events originating from the interaction of the devices installed in

the domicile of clients. Specify about this internal memory in which device

exists, what is its function, and what events does it record, where do they come from, how long

are stored and when they are collected, as well as what devices you interact with. AND

How is the saving produced and with what periodicity, and its destination?

He replied that "the internal memory of the device is located on the motherboard of the

alarm switchboard (Control Panel), its function being to record the events in the

system that are generated and storing only the last ***NUMBER.3

carried out, as indicated in question 4.4.b) (in this proposal 3.4.b).

These records are deleted, cyclically, depending on the new records

that are generated and recorded, so that the generation of a new record

implies the deletion of the oldest of those ***NUMBER.3. Such events can

respond to panel interactions with:

(i) the owners and contacts authorized by it;

the remaining system devices (e.g. volumetric sensors or

(Yo)

photodetectors); either

(iii) the backend of SECURITAS DIRECT.”

The defendant stated that "After accessing the records contained in the memory of the alarm it has been verified that it was connected from the day 11/22/2015 at 11:56 and that there was no anomaly, likewise, the alarm recorded and sent movement detection signals at 8:09 p.m. 11/27/2015, not registering any event afterwards.”

3-14 The claimant stated in the procedure for the exercise of rights TD/00167/2021, that "the request for access to the records contained in the memory They refer to both "the destroyed alarm center and the one that was installed in my housing on 12/5/2015 and that continued to generate signals and records”. For this purpose, it requests that they report on the one that the claimant says was installed on 12/5/2015, if it was within the same contract?, reason why it is installed and what impact does it have on the logs of the destroyed one?, and why weren't the internal memory logs given from said date to 12/13/2015.?

He replied that "First of all, it is necessary to indicate that my client did facilitate that information referring to the logs generated during the period of time indicated in your application, as it appears in the file, in which the two answers are incorporated provided to the Claimant by SECURITAS DIRECT (the first one incorporating a detailed description of the logs and the second by providing the logs as they are collected in the systems of my represented).

In this sense, both the logs

stored in the CRA, such as those coming from the internal memory contained in the switchboard (Control Panel) destroyed on 11/27/2015. Regarding the generated logs from the installation of a new switchboard, the CRA, and therefore my principal, can only access the logs that are transmitted to it from the internal memory of the device, but not those of a merely technical nature that are generated in said internal memory, given that SECURITAS DIRECT only You can access the content of that device in the event that it had occurred an incident that requires your forensic analysis. In this case, given that said incident did not took place, the device remained in Claimant's home until the termination of the Contract, without at any time SECURITAS DIRECT being able to access said internal memory nor was it necessary to carry out any analysis forensic analysis of its content, as there has not been an incident that required it. As It can be verified that these answers do contain information referring to the period mentioned in the question raised. However, it is clarified that said events are incorporated into the document provided by my client as No. 2 to the pleadings to the Commencement Agreement, and generated from the aforementioned day 5 December 2015.

On the other hand, in case of destruction of the switchboard (Control Panel), and always Within the scope of the contracted services, the former is replaced by a different one, being said installation, and the logs generated from the moment of the Installation part of the development of the aforementioned contract. In the case at hand, the reason for the replacement of the switchboard (Control Panel) on December 5, 2015, was due to the damage suffered as a result of the intrusion that occurred on the date 11/27/2015. As already indicated in the answer to a previous question, the logs do not are modified by the fact that this substitution occurs in the device, being those derived from the interaction of the alarm system with the CRA."

3.15 For what reason do you indicate in the appeal for reversal against the exercise of law TD/167/2021 that "in lines of code format" would satisfy in to a lesser extent, compliance with the requirements demanded by the GDPR so that the right of access can be considered adequately addressed"? and what is the format "lines of code", if it is the one of the logs chronologically, without grouping? Input copy of a format lines of code as an example, the one of the fifth access point delivered to the claimant on 02-23-2021 "CRA performance" and indicate what it refers to in the reversal appeal against the TD/00 167/2021 with which the information "was is listed in the table attached to the letter of 02/23/2021", if it is the general explanation of what each column contains or what other information, and where Was it listed?, forwarding a copy of it and if it was sent to the claimant.

It responds that "Given that in accordance with the requirements of article 12.1 GDPR the information provided to the interested party requesting the right of access must be provided in a "concise, transparent, intelligible and easily accessible" manner, and as has already been repeatedly stated in this letter, SECURITAS DIRECT considered that the mere reproduction of the lines of code corresponding to the logs generated by the system, in the format in which they are visible to my principal, I would not allow the Claimant to know the scope, sense and significance of each of the logs sent in response to your request to exercise your right of access.

For this reason, the information was sent indicating the corresponding log, the date and time of its generation and the description of the meaning of said log.

Notwithstanding this, and given that the interested party did not agree with the information provided, the raw information was also delivered and as generated in the SECURITAS DIRECT systems, said information being the one that is collected, shaded in green, in Document Number 2 provided by this part together with its brief of allegations to the Commencement Agreement.”

3.16 The defendant is requested to report how they are similar, and what differences exist among the accesses delivered to the claimant in writings of 02/23/2021, 05/18/2021 and those of 12/14/2021, in terms of quantity and content of logs, and why In the latter and in May, no keys or clear indication of various expressions used in that table.

He replied that: ”As has been indicated on various occasions throughout the present writing, the differences between the two responses provided to the interested is only in their format, containing in both Assuming the same logs. Thus, in the one provided on February 23, 2021, it stated each of the logs collected in the SECURITAS DIRECT systems that contained personal data, including in the first column the times when had been generated and in the third of them a summary description of the meaning of the corresponding log. For its part, in the information provided on May 18, 2021, and subsequently reproduced on December 14, 2021, before consideration of the Claimant that the information provided had not been delivered to him in the format in which it is collected in the systems of my client, the aforementioned was reproduced information, not including the explanatory description of the logs. In this way, each line of the document (those marked in green in Document Number 2 attached to the allegations to the Initiation Agreement) reference was made to an individualized log, being the lines in which said log was repeated were logically similar.

Apart from the aforementioned differences, referring only to the way of presentation of the information, but not its content, there is no difference of any kind additional."

3-17 a) Indicate for the service contracted by the claimant, which logs would be generated when the alarm has gone off, according to the different circumstances that may occur, and what action or actions would be carried out. Indicate the logs that are related with any type of jump alarm that exist in the boxes, and the differences between them, and characteristics taken into account for them to be considered as contain personal data of the claimant or not.

It responded that "the logs generated with the alarm jump suffered by the Claimant on dated 11/27/2015 appear in the document provided by SECURITAS DIRECT together with the brief of allegations to the Initiation Agreement, being understood between the first of those generated on November 27, 2015 at 20:09:47 and the one generated the same day at 8:17:07 p.m. Likewise, the aforementioned document includes the remaining assumptions in which an alarm jump occurred and the logs generated, differentiating those that do or do not contain personal data, depending on whether they are shaded in color green or red and based on the information included in the report that was attached as Document No. 1 together with the allegations to the Commencement Agreement of this procedure. As can be seen, these logs are started by the detection of a volumetric alarm alert at 20:09:47, generating a code random (1155) that is generated with any alarm jump) so that, if it is sent to a guard, he can disconnect it (in this case, it was not used to send to no guard, since it was determined that it was not necessary). From that moment, the system verification logs are recorded for the transfer of information to a operator, who from that moment makes the pertinent calls to those who they appear as designated contacts in the Agreement entered into by the Claimant.

As can be seen, these attempts are unsuccessful with respect to the three first contacts, when the voicemail is sent, communication can be made with the room of contacts which, however, does not provide the word that allows establish communication and that is also previously established by the Claimant in the Contract, concluding the processing of the alert on November 27 of 2015 at 20:17:07 hours.

As can also be verified, all the actions related to the jump of alarm and contact attempts have been considered personal data and provided to the Claimant, not having such consideration the logs exclusively related to with the way in which the SECURITAS DIRECT systems manage and channel the actions to be carried out in these cases or those that refer exclusively to the operator intervener. The justifying explanation of the consideration or not of the information as personal data is contained in the report provided by my client as Document No. 1 together with the allegations to the Initiation Agreement. Also, you can check the existence of different logs related to alarm jumps subsequently deactivated on December 5, 2015 from 18:56:37, all of them having been provided to the Claimant because they are considered to incorporate personal data related to it, given that these are actions aimed at test the operation of the system installed in your home, carrying out different alarm tests (volumetric, seismic, duress or magnetic). I also know produces an alarm jump on December 6, 2015 at 01:15:04 hours,

being able to check the logs generated by the system, and which concludes with the

communication with the owner indicating at 01:17:22 hours that the alarm jump

it may have been generated by the chimney.”

a) In the requested access, inform if, as a result of any alarm jump, it was

communicated to the Police the possible access to the property, and if it is registered in

logs, indicating which one it would be.

He responds that "communication with the police generates the corresponding log, which in

this case was not generated because that contact did not take place.”

Likewise, report if the logs contain any "unconfirmed alarm" event,

b)

indicating what they would be and if personal data has been considered.

"In the response given to the first of the questions contained in this section, it is

they have indicated the alarm jumps produced and their vicissitudes. The explanation about

whether or not the generated logs contain personal data is included in the document

No. 1 attached to the allegations to the Commencement Agreement.”

3-18-If when an alarm jump occurs, all the actions related to

with the device remain in the logs and if additionally, they can be generated or created

others by the operators themselves, and what they would be, indicating if they would all be data

personal, or not, and the logs of each one of them (if personal data of the claimant,

No).

He answered that: "in the answer to the previous question, the jumps of alarm produced in the Claimant's system with the generated logs, being able to differentiate between those that do or do not contain personal data. Likewise, as already has indicated, the logs generated by the system are not left to the discretion of the users of the same or of SECURITAS DIRECT personnel, being those previously constituted in the system, although logically the actions of said personnel give rise to to the generation of the corresponding previously configured logs."

3-19 a) Regarding the protocols that Securitas must carry out voluntarily - checks and technical verifications, and related to system maintenance, specify the articles and the specific norm that regulates them, periodicity or motu proprio, the protocol internal summary of actions carried out by them, and if the regulations of application provides for monthly activity reports for each alarm for the owners, if these reports are fed from logs extracted from the registry of the device.

He answers that: "First of all, one must start from the difference between a revision and a maintenance to which reference has already been made in the answer given to the question included in point 4.8 "(in this proposal 3.8) of the writing of that AEPD. Starting off of said base, revisions and maintenance are regulated in articles 43 to 45 of the Private Security Regulations and in article 5 of Order INT/316/2011. In They refer to the periodicity of the reviews, as well as the way in which face-to-face and remote reviews must be carried out, both in accordance with the Annexes II and III of the aforementioned Order. The verification tests of the correct communication and transmission of the alarm, is a test that must be carried out depending on the the characteristics of the property, based on its different risk of robbery or intrusion (so, for example, in a jewelry store there is a greater risk, so the systems alarm must have periodic communication tests with a periodicity less, than in a system installed in a private residence). This aspect is

It is also related to the degrees of security and the certification of the

systems in accordance with the UNE or UNE-EN standards that are applicable. In addition,

Article 45 of the Private Security Regulation regulates the delivery to the holders of

the installations of a manual of use and preventive and corrective maintenance that the

The user himself must carry out, including actions such as changing the

stacks of devices, control over object placement that prevents uptake

detectors, etc. The regulations do not regulate the obligation to send reports of

alarm activity, so that each company determines if the alarm is carried out.

periodic sending of this information. In addition, the client can consult in the App the

connections and disconnections that you have made with the different keys placed at your

provision. The only case in which the submission of a report to the holder of the

contract as well as to the Security Forces and Corps, occurs in the event that

a confirmed alarm jump has occurred and it has not been transmitted to the

Security Forces and Corps, in which the reasons for the

that this transmission did not take place."

b) In their allegations they indicate: "Securitas generated logs until 20:09 on the day

11/27/2015, time and date on which the intrusion into the residence of the

claimant and during which said alarm system was completely

disabled from that date could not generate more logs". However, in the annex

I, which includes the logs, contains logs after 11/27/2015, 8:09 PM. How I know explain this fact? And what is the origin and purpose of these logs, and why not them? considered personal data of the claimant.

It responds that: "The logs generated from the moment the jump of alarm, and once those related to attempts to communicate with the the contacts designated by the Complainant, refer to successive attempts to communication between SECURITAS DIRECT and the system installed in the domicile of the Complainant, which were unsuccessful and being machine-to-machine interactions of a technical nature."

3.20 Explanation of why there are logs with different signs, according to what was provided, considered personal data or not, and within these more than one, which coincide in the exact recording of the time, example in the Excel tables provided in allegations appears as non-personal data, 11/27/2015, 20:09:47, volumetric alarm. Intrusion volumetric, seismic-according to panel version. Devices that do not need restoration V8.8 to 9.5)- volumetric intrusion radius Volume, and the log of the day 12/5/2015, 18:56:37/ALARM/URGEN/XPO09 RP-Perimeter alarm SER Volumetric-photo. Volumetric intrusion, seismic-according to panel version. Devices that don't need restore V8.8 to 9.5)-

Answer: "As already indicated in the answer to the question raised in the section 4.17" (in this proposal 3.17) "of the letter of that AEPD, the two logs mentioned therein differ in terms of their content, given that in the first of the assumptions a volumetric alarm jump of unknown origin occurs, that does not provide information about the interested party, Claimant, while the The second is due to the performance by the former of various tests in the alarm reinstalled by SECURITAS DIRECT, deducing from it the existence of personal data of the interested party, which generates the jump of the alarm system in order to verify its proper functioning.

3.21 In the table that was given to the claimant on 12/14/2021, as well as in document 3, green table that you provided in allegations, and which are personal data, there are various codes in the columns, numerical, or letters, without which it is not clear information. You are asked if the creation or collection of the meaning would be possible of these keys, which appear in almost all the columns.

He replied that: "Regarding the alphanumeric codes that appear on the "SIGNAL" column, it is the message generated in the system's own language alarm that is translated into the information that appears in the rest of the columns and essentially in the column of "***COLUMN.2 (...)".

Therefore, to understand the meaning of the code, one must go to the field of column "***COLUMN.2 (...)". The system sends messages that incorporate codes alphanumeric codes that are later translated into the different columns of the Log presented. The "SIGNAL" column collects the part of the "raw" message from the system, in their own language (machine language) which is then translated into the rest of the columns.

For this purpose:

• The column "***COLUMN.2 (...) is the translation of the system language event to technical language, so that the agent/operator understands what the message is about. This information is complemented by the columns "***COLUMN.1" and "***COLUMN.2" that contain complementary information so that the agent/operator can understand the event that is received at the CRA.

- The "ZONE" column identifies the alarm device in which the alarm occurs.

event (eg (...), identifies a recording photosensor in programming position 2) and

the “AREA” column describes the zone of the installation that corresponds (eg, Home

living room)

- The column “***COLUMN.3” indicates the priority of the signal, being the values

lower priority ones.

- The column “***COLUMNA.4”, contains the type of signal that represents the event

(e.g. INF is the code that is associated with "information", which appears in the

***COLUMN.2 (...), SS is associated with “supervision”, as also included in the

***COLUMN.2 (...), CC is associated with “coercion”, SO is associated with “SOS”, AAC is associated

to “power outage”, etc…). In this way, these codes are directly linked

with the information contained in the column ***COLUMN.2 (...).”

3.22 In the report of 01/29/2021, provided by the defendant in allegations,

document I, table II, containing personal data, provided in their allegations,

the entry is recorded: 12/05/2015 14:19:04/REGISTERED ACCESS: The user

***USER.1 accessed the file of the client/Internal registration of the operator who is

acting on a specific incident/ Information related to a character operator

procedural and internal Securitas Direct / personal data is considered: YES / If applicable

would be considered personal data of the operator itself and therefore would not be

capable of being provided to the interested party requesting the right of access.

You are asked to answer who the mentioned user is, and if you access the file of the

client, is related to their data, or accesses from the time the alarm is

working, why shouldn't they be provided? In fact, in the access

has provided you.

Answer that: "As already indicated in the answer to the question raised in the

section 4.6 of the document of that AEPD, "(in this proposal 3.6)" the reference alphanumeric to the user refers to the registration of the same in its condition of employee of SECURITAS DIRECT, maintaining this information pseudonymized to so that its disclosure to the Claimant does not imply a transfer of the data of said user, since access to the Claimant's customer file does not imply the processing of personal data of the latter, but only of the employee who accesses such information. The data has been provided to the Claimant in order to deliver to the Claimant all the information that could be possible to provide without, therefore, harming the ordinary activity of SECURITAS DIRECT nor the information that would be found

protected by trade secret. However, it is reiterated that the aforementioned log does not releases any personal data referred to him. In this sense, it is reiterated doctrine of the AEPD by virtue of which the right of access does not include access to the information referring to the specific users of the data controller who have accessed the personal data of the applicant."

3.23 In the same report and same table of the previous case, there is the log of 12/18/2015, 20:08:18 ***COLUMN.1 Logged: B.B.B., explain that "The record of actions of a user supposes the obtaining of personal information about it. If it's about of a personal data of a third user other than the exerciser of the right of access and, therefore, it would not be possible to provide the interested party requesting the right to access", as they know that under this log it is not the owner who exercises the right, reason then for which it appeared in the table delivered to the claimant on 02-23-2021 (There are others with the same reference).

Answer that: "As a prior consideration, it must be ruled out that the person to whom referred to in the aforementioned log is the applicant for access, not corresponding to the Claimant, nor with any of the persons authorized by the claimant as contacts in his contract, as can be seen from the identification made in the matter raised. Having made this consideration, we refer to what is indicated in the answer given to the question raised in point 4.6 of the letter of that AEPD." (in this proposal 3.6).

3.24 In document 2 presented in the registry named in allegations "confidential client total logs", which contains the logs in red and green, you are prompted to clarify, because:

The notice appears as no personal data in red:

11/27/2015 20:09:47/comment volumetric alarm/intrusion description volumetric-seismic according to panel version devices that do not need restoration v 8, 8 to 9.5 volumetric intrusion radius.

In table I (report of 01/29/2021, provided by the defendant in allegations) the log is also contained.

It is requested that they report if the alarm was activated by the owner and the following occurs that appears in the information "radio volumetric intrusion", why don't they consider it personal data, by being related to information, last configuration made, or that it could have been by the owner or another user?, and what relationship does it have with the next one that appears in green, as personal data, is the same date and time, with different codes, and with another in red, same date and time "description level of panel coverage"

In addition, it is observed that the same description appears in green as data personnel on different dates from the same chart, example 12/5/2015 18:59:08, 18:59: 27, 18:59:48 18:59:57.

Answer that: "As described in the answer to the question incorporated into section 4.17 of the AEPD document" (in this proposal 3.17) “the information marked in red responds to a technical event in which there is no data any personnel of the Claimant (in this case the detection of an alarm jump) and Therefore, it is not part of the information that must be delivered in the case of attention to a request to exercise the right of access made by the aforementioned Claimant, in accordance with article 15 of the GDPR. This is indicated in the report provided by my client as Document No. 1 attached to the writ of allegations to the Commencement Agreement (page 25) the following: This log line, although provides information about an alarm jump in the sensors, insofar as the that direct information on an attribute of the interested party is not transferred, nor is Securitas Direct is intended to analyze a pattern of behavior or influence it in any way, the information provided by the analyzed log line should not be considered as personal data. In this sense, it would be a description of the technical and internal Securitas Direct.” The remaining logs generated on that date and time have been provided to the Claimant when they include personal data that could refer to it, not being provided in the event that they are events merely technical, following the content of the aforementioned report (see pages 23 to 26 and 36 to 38 thereof). The logs generated on 12/5/2015 to which this question do not derive from an exclusively technical event, but from the interaction of the user with the system, triggering the alarm to check its operation, for which they effectively reveal personal data of that person and for this reason they have been delivered to the interested party when exercising their right of access, as well as described in the response to the question raised in section 4.17 of the letter of that AEPD." (in this proposal 3.17).

3-25 a) Clarify document 1, table I, logs of non-personal data, from the 01/29/2021, provided by the defendant in allegations, what does it mean or to what reply:

"Logs, 12/06/2015 1:17:12, 12/06/2015 1:17:26/ NO REASON N/A Not provided information regarding any characteristic, pattern of behavior, or other user information. NO"(p. 26/105)."

Answer that: "As indicated in the answer to question 4.17" (in this proposal 3.17) "the cited logs respond to a technical incident, which gives rise to an interaction with the owner from which it can be deduced that said incident may have be caused by the chimney and that there is no anomalous situation. Are interactions have been communicated to the interested party in the response provided to their Exercise of the right of access."

Despite the response, it can be seen that the logs appear in red in document 2 of allegations to the initiation agreement.

-Table I, after the previous one: all grouped in (...): 0 "27/11/2015 20:11:34 ,12/04/2015 11:04:50, 12/05/2015 9:30:10, 12/05/2015 10:48:31, 12/05/2015 13:14:21, 12/05/2015 14:17:44, 12/06/2015 1:15:22, 12/06/2015 16:33:51, 12/09/2015 8:54:14, 12/15/2015 2:38:08 12/15/2015 4:54:57"- Indicative that the incident was transmitted to a human or machine operator. The signal, given its relevance, is transmitted to a machine or human operator to start the management process. No However, it is an internal procedure from which no personal data can be inferred. of the user. NO". It is requested to clarify the key meaning (...):0, what would be the incidence?, Does the signal come from the home alarm switchboard? And why doesn't it say that

incident is treated and does not clarify defining who is transmitted.?

It responds that "The callsign (...):0 is limited solely to recording in the system,

(…),

as indicated, that there is a

well to an employee so that

carry out the actions that are established based on the event that has caused it

generated, either to the system itself, to carry out the verifications

(…)

coming. Thus,

, but exclusively the internal procedure

followed by SECURITAS DIRECT in the event of an incident that appears in a previous log, with

the one that can coincide in the generation time, given the automaticity with which

Opera

."

3-26 -in table I, of non-personal data, Logs existing between the dates:

a) 11/28/201 22:21:18 and 12/04/2015 9:04:26

b) 12/04/2015 11:08:02 and 12/05/2015 13:16:56

c) 12/06/2015 16:33:51 and 12/06/2015 16:33:57

d) 12/15/2015 2:38:08 and 12/15/2015 2:38:12

e) 12/15/2015 4:50:38

f) 12/15/2015 23:24:51 and 12/16/2015 12:20:34 / (...) transfer, “Also, the logs describe the internal and technical actions carried out as a result of this disconnection”

Report how and by whom this procedure is initiated, and before what event is usually produce

Answer that: ”As also indicated in the answer to question 4.17” (in this proposal 3.17) "of the writing of that AEPD, these records are derived from the signal that the system performs automatically to verify that it is finds operational. As there is no response from the system installed at the home of the holder, the logs to which reference is being made are generated, being able, from that log automatically open a maintenance procedure, so that a technician proceed to repair the device if necessary. In this sense, as appears in the information already provided, on December 4, 2015 at 11:25:04 mi principal communicates with the authorized contact number 2 of those designated by the Claimant in his contract that indicates, as stated in the documentation, that my principal contacts them the next day to carry out tests according to COM LOG that we call the next day for tests. for this reason, the aforementioned communications of December 4, 2015 do contain data personal and have been delivered to the interested party as a result of the exercise of your right of access” It is appreciated that the log in which you contact no. 2, the 4/12/2015, could be the one at 11:06:07

3-27 Since the log can indicate that an intrusion is detected and gives information about alarm jumps, which is why the log of 12/6/2015 1:15:04 and those grouped in PHOTO RADIO intrusion in table I of document 1, it is considered not to be data personal, it is not indicating that they give the data of the image, but the information of that there has been an intrusion, and why it would not be personal data said information.

It is also observed that a log with the same date and time appears as personal data, in green in document 2 of allegations agreement start, although with another description: "code to disarm the alarm" "Central high priority" In other instant logs later figure "everything is fine", "indicates that it could be the chimney" interspersed with other red logs, no personal data, about "panel coverage, images so that CRA downloads them or "images already in CR".

Answer that: "As indicated in the answer to question 4.17", (in this proposal 3.17) "the cited log responds to a technical incident produced in a photodetector which, in the claimant's judgment, had been generated by the home chimney. This incident gives rise to a volumetric alarm jump, that is, that is, an intrusion or anomalous event is identified, and the contract holder may access the generated photograph through its App."

3.28 a) same table and document mentioned above, logs from 12/15/2015 2:42:11 and 12/15/2015 4:50:19 ELECTRICAL CURRENT (AUTO) Detection of lack of electrical current in the device. Securitas technical information direct. To the extent that direct information about an attribute of the data subject nor does Securitas Direct intend to analyze a pattern of conduct or influence him in any way, the information provided by the parsed log line should not be considered as personal data. Indicate what the denomination implies, and if the device was (...) by the owner, because this log would not be considered information of its owner since it could affect his right.

Answer that: "The log to which this question refers has an exclusively

technical and is limited to detecting the existence of a cut in the electrical supply that

affects the device. SECURITAS DIRECT cannot know the reasons why

which the power failure has occurred. However, the system remains

operation, since it is equipped with an auxiliary battery that allows its

supply when the alarm is armed in order to identify the

incidents that could occur during the cut produced. For this purpose, it is

irrelevant who and under what circumstances proceeded to the

, given

that the only thing that the log reflects is the existence of the absence of electric current in

the device, so that no natural person can be identified by the

occurrence of this event nor does it provide any information about a person

identified or identifiable. This incident generates the remission of a communication to the

owner, indicating that the (...) system has been modified as a consequence

of the aforementioned cut, as can be verified in the documentation provided

by my client The log generated by said communication does contain data

personal data, and this is reflected in the document sent to the interested party (logs generated on

day 12/15/15 at 4:50:24 that appear in the document sent to him)."

(...)

alarm system

It is observed that in the logs of that day they begin with annotations of no data, in red

at 2:38:07, four logs, and the next one at 2:38:23 if it is a personal data log, with

information (...)

and at 4:50: an e-mail sent to the claimant's address,

continuing to include several logs of non-personal data with references to "failure supervision”, “incident cancelled, maintenance pending”.

-b) because in several of these logs in Are they considered to be personal data?, they indicate

As a general rule, no, but images are collected when they are detected

movements through the sensors, in case they had captured the interested party,

would be personal data and should be provided to him, and how do they know that the person

who accesses is the owner, an authorized person, another user?, and if, should not inform the owner

from the fact that images have been collected, if anything.

He answers that: "In relation to these logs, not all the sensors installed in the

Complainant's home include photographs (e.g. at that point reference was made to

volumetric sensors).

In any case, SECURITAS DIRECT can know if the image, if it is

collected if an alarm jump implies the development of the corresponding protocol (see,

for example, the response given to point 4.17 of the letter of that AEPD)” (in this

proposal 3.17) "which involves communication with the person or contacts

designated. In this way, if from said communication it is derived that the image is

refers to the interested party, a copy of the same would be provided, which would also be

accessible by him from the App.”

3.29 What does the extended description that appears in a table consist of as

"Internal registration of the operator that is acting on an incident".

Answer: "It has already been indicated in the answer to the question contained in point 4.6"

(3.6 in this proposal) "the internal registration of the operator that is acting in a

incidence" is the internal alphanumeric code that uniquely identifies the
SECURITAS DIRECT employee who is working on the device to
solve or manage a technical incident that occurred in it.”

3.30 What are they referring to when they state that the system performs
“Autonomous system checks that are performed without user or intervention
nor the service provider", and object, between which equipment is produced and if it appears
regulated in private security regulations or in its own protocol and that can
assume its non-performance.

It responds that: "For "Autonomous verifications of the system that are carried out without
intervention neither of the user nor of the service provider", and following what is stated in
question 4.8” (in this proposal 3.8) “we were referring to the tests
periodic communication and correct transmission of the alarm system with the CRA.”

3.31 a In annex II, information, they indicated that:

- "Those log lines not derived directly from the results have not been analyzed.
security system services provided by Securitas (i.e. logs with
designation: FR0 to FSZ; ROF and ROI). Likewise, they have not been subject to
I study those log lines that, according to the information provided by
Securitas, have no practical application as of the date of writing this report:
IAC, ICA, PID, PDD, TLL and TWC”. Explanation of the meaning of this is requested
annotation.

Answer that: "The meaning of these expressions refers, as the content of the own report can be deduced, to logs that no longer operate in the SECURITAS DIRECT or that are not related to the operation of the Claimant's alarm, so they do not fit what was requested by the Claimant."

b) There is a log that indicates: “VCA/ Available Photo/Video Alarm in CRA Images already in CRA./ …Notwithstanding the foregoing, the captured images, in case they had captured a subject, it would be personal data and should be provided to the interested party provided that the applicant for the right of access coincides with the person captured in the images./ Personal data is considered: Yes. Explain why if the images captured by the owner himself when the alarm was detected, said images will not

They can be transferred to the owner of the device, including if they are their own.”

He replied that: "In relation to the delivery to the interested party of images captured will have to differentiate:

(Yo)

the situation in which the person who appears in the images is only the applicant for the right of access, in which case they must be granted together with the the rest of the relevant personal data and,

the situation where the device captures images from a third party, in which case

(Yo)

could not be granted with the right of access as it would imply a communication of personal information. In this sense, the criterion supported by SECURITAS DIRECT would coincide with that established by the AEPD itself in relation to the exercise of rights in relation to video surveillance systems. Thus, in section 2.3.10 of its Guide on the use of video cameras for security and other purposes indicates that this right "has unique characteristics, since it requires contributing as complementary documentation an updated image that allows the person in charge verify and verify the presence of the affected party in their records. It turns out practically impossible to access images without compromising the image of a

third. For this reason, access can be facilitated by certified writing in which, with

as accurately as possible and without affecting the rights of third parties, specify the

data that have been processed”. In any case, the holders of the

SECURITAS DIRECT alarm systems have access, through the App, to the

images captured by the devices at the time an incident occurs

by jump alarm by means of a device capable of capturing images.

Likewise, these images are made available to the Corps and Forces of

State Security if necessary. In any case, the possible access by the owner

of an alarm system to the images, without prejudice to its legality as a transfer of

data, would not form part of the right of access of the interested party, as

It follows from the doctrine of that AEPD that has just been reproduced, by not referring to

your own data

b) Explain the meaning of this log: “SID Inactivity time Periodic verification of

movement within the home. From the joint information provided by: (i) the

time without motion detection; and (ii) date of the specific log in the case of a

analysis of a real log, knowledge of certain patterns of

behavior of a user, so this log line could be considered as data

staff. YEAH.

It responds that: "The report provided as Document No. 1 attached to the allegations

to the Initiation Agreement, not only analyzed the specific logs generated in relation to the alarm system contracted and located in the Claimant's home, but the all the logs that an alarm system could produce, including those which in no case occurred in the controversial case, since my principal wanted to know the scope of the application of the concept of personal data in the operation of said alarm systems. For this reason, the report differentiated in three tables the logs generated in the specific relation of the Complainant with SECURITAS DIRECT, distinguishing those that would be considered data personnel (table 1 of annex I) and those who do not (table 2 of annex I), as well as the rest logs that could be generated by any alarm system, analyzing whether they whether or not they fit into the concept of personal data (Annex II). The log to which this refers question is not among those generated in the case of the alarm system of the complainant, so it can be considered that the question raised is irrelevant for the purposes of this file.”

3.32 If it is possible that the logs overlap, existing for example the one that is registered the (...) alarm by the owner and subsequently others have been registered events.

He responded that: ”Each log line is a unique record with date and time, and even there can be several in the same minute and second as they are "machines" but this It does not suppose an "overlay", but the generation of several simultaneous logs."

3.33 a) It is requested that they inform if the table can be provided to the claimant ANNEX II containing the (...) of the signal and the descriptors, (report of 01/29/2021, provided by the defendant in allegations) and reason in case it was negative.

It responds that: "Annex II refers to logs that have never been generated in the claimant's alarm system, so that said information in no way case would be related to your Contract, regardless of whether or not it had the character of personal data. At the same time, as has also been shown manifest in the allegations to the Initiation Agreement, the operation of the systems

of alarm of my represented and the logs that they generate constitutes an asset of

SECURITAS DIRECT protected by the rules that regulate trade secrets. Of

this way, the information being irrelevant to the interested party and being, for

On the contrary, my principal, protected by trade secret, considers that neither the

regulations for the protection of personal data, nor any other authorize that

have access to that information.

It is appreciated that Annex II, called "general analysis on the consideration of data

staff" found in document 1 provided in allegations to the agreement,

contains a letter key called “(...) of the signal” which also appears in the box

of document 2, signs in green, data of the claimant, and that it coincides with the

format delivered to the claimant on 12/14/2021. By way of example, it appears in both

annex II as in the table delivered to the claimant: IDE, the description of the signal

“External disarm”, as well as the extended description provided by SD and a

explanation of linkage directly or through inference to behavior or

information of a natural person, and YES in personal data, so it would be

explanations that have to do with the content of what has been provided to you

b)-Reason why annex I, tables I and II, does not contain the key (...) of the signal and

its description that is contained in the table of ANNEX II

He replied that: "Reference must be made again to the scope of the report to which

this question refers to, in which it was possible to differentiate the logs actually generated in the Claimant's system of those that had not been generated, so that while the first could be differentiated according to the moment in which they were produced, the seconds could only be referenced by a specific denomination. that and no other is the reason why the tables of both annexes differ, in the same way that the tables contained in annex I indicate whether or not to include the corresponding log in the response provided to the request to exercise the right of access, which for obvious reasons does not appear in the table in annex II."

3.34 In the event of an alarm at home, to whom would the information?, to the last user that appears logged in in the alarm connection?, to the headline? Under what assumptions? And how do you identify them in the logs? -Detail in this case, some log that considers personal data and that motivated by the alarm jump, is have given information to that person.

Respond that: "The action protocol in the event of an alarm jump, and that was followed in the case of the Claimant in the alarm jump dated 11/27/2015, it is the next:

- Call to speak/listen to the alarm center. (Audio Verification).
- Call to the landline telephone of the home where the system is located, if have that data.
- Call the designated contacts in the order established by the holder of the contract in the action plan that appears in the Contract and verification of the word clue.
- Contact information in case of communication with it and the keyword verification.
- Notification to the Security Forces and Bodies in the event of indications evidence of the possible existence of a crime (in the case of November 27, 2015 was not executed because it was not considered a confirmed alarm).

"In relation to the specific assumption analyzed, as described in various previous answers, the interested party designates in the Contract up to four contacts, also establishing an order of priority in the communication to them of a certain incident. Once you get in touch with one of the contacts designated, you are prompted for the password, without which you are not provided with the information about the identified incident. This is how it happened in the alarm jump produced on November 27, 2015, in whose logs it can be seen how attempted contact successively with the persons designated first, second, and

third place, being unsuccessful, and since the contactee in fourth place did not facilitate the keyword."

3.35 In their allegations to the initiation agreement, they indicated that:

"After presenting the information, the Agency also mentions the" time jump between 11/27/2015 at 8:17 p.m. and 12/4/2015 at 11:05 a.m., without explaining the reason for that absence of “logs” in that time interval”. On this statement you cannot this part but to state, said without the intention of offending the Agency, that it is not corresponds to reality and it is enough to refer to the document presented by this party to the Agency on 06/18/2021 (pages 106 and 107 of the file) where my represented shows (we quote verbatim what was stated by SECURITAS DIRECT) "it generated "logs" until 8:09 p.m. on 11/27/2015, time and date on which the intrusion into the claimant's home occurred and during which, said alarm system was completely disabled. from that date, it could not generate more logs”. In addition, and in relation to the internal memory of the device, this party also revealed in its letter of 06/18/2021 (pages 106 and 107 of the file) "(...) after analyzing the internal memory of the installed alarm only had a "log" generated for that time frame, which It was recorded in our burofax dated 02/26/2021”.

a) Note that there are logs in that period that are considered non-data personal. In this regard, you are requested to indicate how such logs are started and how end.

They respond that: ”As has already been indicated on several occasions, the logs to which the question refers to correspond to those generated directly from a SECURITAS DIRECT operator at the CRA, and basically consist of the successive attempts to communicate with the interested parties to report the incident and check the alarm status. It is not about the communications from the switchboard located in the claimant's home, which, when rendered useless, could not generate no type of log or signal, as evidenced by the logs that the system generated between 22:21:18 on November 28, 2015 and 11:04:50 on the 4th December 2015, to which reference has been made earlier in this written."

to)

Also explain how the interruption is linked to the first log of resumption, (cataloged in green) 12-4-2015, 11:05:04, what event produces it and what personal information would provide this.

Answer that: "The aforementioned log is the result of technical verifications through an automatic system called GTI (as it appears in the log itself) that is is in charge of carrying out various checks to know the technical state of the system, proceeding to the opening of a maintenance when necessary. In

In this case, an operator is in charge of calling the client to make a review with the customer online and if this is not possible, arrange a visit by a technician to verify the system state”.

It can be seen that on 12/4/2015, as in previous days, the logs appear in red, while as of 11/28/2015 they are all in red.

3.36 a) In document 2 of allegations, -total logs- Excel table of all logs, differentiated in red-no data-, green, yes, figure:

With different keys of the "(...) of the event" distinguished in red those considered not personal data, example, there are two in red, from 11/27/2016 20:09:47, and another one date and time, in green. How are they similar and how are they different in terms of the references of its contents in terms of information on personal data that can contain.

b) In this case, for example, detail the difference of these two logs (of no data personal) in terms of origin and because at the same time, in this case, one does considered personal data and the other not.

Likewise, if you wish, comment on other logs -not personal data- that coincide with the date and hour.

Answer that: "As stated in the response to the question contained in the point 4.17” (3.17 in this proposal)” the logs refer to different events: the first involves the detection of an alarm jump detected by a sensor volumetric; the second involves the generation of a deactivation code in case that it is necessary to go to the house once the verifications have been carried out

corresponding, which also appear in the logs table; and the third refers to

the coverage (...).”

c) Explain if it seems possible that as it happens with the marks of the non-data logs

personal that there may be more than one on the same date and time, if you could also

there should be two of the same date and time so that logs of those considered

personal data, some example, and if in those of the claimant it occurs in any case.

Answer that: "The answer to this question would be that it is possible and an example of

These are the following logs marked in green that refer to maintenance

alarm change presence. There are several logs that occur at the same time

temporary. 12/05/2015 18:38:10:”, indicating four movements of the same date and

hour.

EIGHTH: On 02/2/2023, a proposal for a resolution of the literal is issued:

"That the Director of the Spanish Agency for Data Protection sanctions

SECURITAS DIRECT ESPAÑA, S.A., with NIF A26106013, for a violation of article

58.2 c) of the GDPR, in accordance with article 83.6 of the GDPR, classified as very

serious in article 72.1.m) of the LOPDGDD, with a fine of 50,000 euros.

In accordance with article 58.2.c) of the GDPR, it is proposed that compliance with the

right of full and understandable access, as specified in the last foundation of

law and follows from the meaning of this proposal.”

NINTH: On 02/20/2023, the defendant made the following allegations:

A) About the technical logs and their assimilation with personal data, states:

1-The device will at no time be under the influence of the claimant, nor would it have ability to exert influence over the claimant since he does not have the ability to configure or modify the technical parameters that affect the mode of operation and the configuration established by SD for its interaction with the receiving center of alarms.

2-"Although the number that identifies the device in relation to the contract entered into with a certain client must be considered personal data when linking with the party in said contract", the interpretation carried out by the AEPD in its proposal distorts the concept of personal data, and, consequently, the application of the GDPR, understanding that each technical action on that device is a personal data of the claimant, it is that is, that it constitutes information "about" him, and that, therefore, must have been provided in the right of access.

- The information in the technical logs has no impact on or on the interested party, nor if-want indirectly, as they are signals and communications carried out between machines that, in any case, they are unrelated to the owner of the home on which the system is installed and They do not affect it, directly or indirectly.

3- Reiterates the meaning of Opinion 4/20007, on the requirements that should be met in the information to understand that it can be considered personal data, when it “be seen on an identified or identifiable person”. In the framework of their discussions on data protection issues raised by RFID tags, the Group of work pointed out that a «data refers to a person if it refers to his identity, and their characteristics or behavior or if that information is used to determine or influence the way she is treated or evaluated.”

To consider that the information referring to a specific object, the alarm device, installed in the claimant's home may be considered personal data, as it relates to about a person, there must be an element of content, or purpose, or result.

In the report provided in the initiation agreement it was already indicated:

 The information must refer to a specific natural person, so the information

in the logs must, at least, be in one of the following situations:

a.1 Be directly linked to a specific individual, in such a way that

provide direct information about their way of acting, their mental characteristics or

physical features, preferences, abilities, or any other pattern of behavior that may

be directly attributed to it, or

a.2 Can be used to evaluate or influence in any way a particular individual

or in his conduct, or

a.3 Can have a direct impact on the rights and interests of an individual

certain.

From this conclusion, it was inferred that the technical logs could not be considered personal data.

personal because it refers only to an object and is not found in any of the sub-

mentioned positions.

The evaluation of the proposal only alludes to the fact that technical logs are personal data

due to the fact that they are linked to the alarm system identifier, and this, via contract

to the claimant. It considers that the "content" requirements do not meet: It does not provide

information directly about the interested party, of the "purpose": the objective of the

technical logs is not to evaluate, treat in a certain way or influence the situation or

behavior of a person, nor of "result": that "would occur if the use of the information affects or could affect the rights and interests of the claimant" , "since there is no possibility that through the information obtained from technical logs may in any way affect the rights and interests of the interested party that is not related in any way to the operations that constitute said logs”. The “use of this information could imply differential or discriminatory treatment of the interested party or an affectation in his personal sphere”.

4- The consideration as personal data of the information contained in the technical logs is not affected because it refers to the ARC-alarm device interconnection installed in the domicile of the claimant, since the purpose of this, in nothing can determine the nature of the personal data or not of the signals that it emits. Whether follows this reasoning any information related to an object could lead to consider it as personal data, when its usefulness or purpose is affected for which it has been acquired or is derived from a service contracted by the interested,

In addition, it considers that information related to machines or systems has no necessarily the condition of personal data in case they do not reveal information about an identified person.

He gives as an example the mixed data (personal and non-personal) that can be inextricably linked or not, being able to enter the scope of the right of access, or No, which means that only the personal data in the group is accessible to the user. interested party, as stated in the EDPB guidelines 1/2022 on the right to access. It ends by indicating that these circumstances can be extrapolated to the present case, in which the internal operation of the device and its interaction with the CRA, without incorporating more information than is relevant to verify and analyze the operation of the contracted alarm systems.

Regarding compliance and its manner, regarding the claimant's request for access, states:

1- Regardless of the consideration that one has about the nature of personal data of the

technical logs, which is not the object of this allegation, the excluded information does not have the

character of personal data, having been given access only to what refers to the

personal data processed by the person in charge receiving the request.

2-Has tried to respond to the claimant in the terms that the claimant has requested, and

even facilitate the understanding of the information provided. It was the claimant who,

once information was provided that was intended to clarify the scope of each of the logs

provided considered that what should be provided were the "raw" logs, without the

grouping and clarification previously carried out, to later consider that this

The information did not satisfy him either, as it was, in his opinion, not very understandable. Which

pursued by the claimant is the information generated by the alarm system, given that

understands that there was a failure in its operation that led to the theft in its

property

B)

Regarding the disclosure of "know how", he states:

1-Law 1/2019 of 02/20/2019, on business secrets, aims to guarantee and

protect undisclosed know-how and business information from

its illegal obtaining, use and disclosure. In this case, it has lace as

information being referenced, which reveals internal processes and the

mode of operation of the installed alarm systems and in consideration of the article 1.1 of said Law

2-The information of its systems and processes constitute an asset. The security that can communicate with the technical logs must be adequately protected to avoid access by third parties that could circumvent or circumvent the operation of said systems.

The information that is provided in the logs contains an informative activity and recorded through their own information systems (i.e. current status of programs, security, access, network connectivity, etc.), and therefore, said information results generate a standardized work methodology that is owned by SECURITAS DIRECT.

Links the disclosure of this information to the safety of users of your systems alarm, as a guarantee of the general interest and the preservation of security that It affects all the generated logs. It considers that the individual right of the claimant cannot prevail over the guarantee of the integrity and security of all Your clients.

3-Employees have access to the information due to their employment relationship, and it lacks relevance what is indicated in the proposal, as it is left out of the application of the regulation of business secrets, whose effectiveness is external to the company. “The logs used in the devices owned by him, provided to the Claimant, contain non-personal information that, used automatically and in aggregate, provides a series of signals that, studied in aggregate form, provide SECURITAS DIRECT relevant and proper information for the improvement of services security that provides, in addition to describing, in its sequential reproduction, the internal procedures followed by the systems of my client, whose disclosure to third parties could produce an impairment of their rights.”

4-The "trade secret" to be protected does not come from the study of a single log (remember than without data processing), but said "commercial secret" comes from the study set of all logs, which allows SECURITAS DIRECT to be able to anticipate events that may occur and affect the safety of its customers,

being able to adopt the measures and guarantees that derive from the study and analysis of those logs.

5-Of the technical logs, only common technical and algorithmic measurements are observed to all devices, used together to provide users with a high level of security in the service provided. He considers that "it is not appropriate the disclosure of its know how, by providing logs that are used in a manner exclusively to provide the service it offers to all its clients, since to do so, you would not only be placing yourself at a disadvantage with the rest of your competitors, but that, what is much more serious, the right to personal integrity of its clients and those who reside with them, although we consider at least similar protection to the right to the protection of personal data."

6-In addition, on the legal basis X of the proposal, it is deemed necessary provide the description of the processes through the keys that allow to clarify the mentioned table and its sections that make the tables of the data understandable in line or raw format, as obtained by the defendant, which considers that multiplies the risk of harm for all its customers. He believes that in order to "guarantee the integrity and proper functioning of its services, considers that it cannot provide the claimant with all the logs, since doing so would be jeopardizing the safety of more than a million and a half customers who hire

its services".

7-Consider that the trade secret of your rights is much more relevant, for

general interest and the preservation of security.

C) By virtue of the aforementioned, he requests the file of the imputation. Besides,

Regarding the graduation of the sanction, it states:

1-On the application of article 83.2.a) of the GDPR, based on the fact that it is confused

what is an element of the sanctioning type with an aggravating circumstance and the

indicated circumstances are taken into account to delimit the alleged infringement, as well as

as if to aggravate it, "which violates all proportionality."

2-Considers that the information provided is neither incomplete nor a mere

“summary with sparse information”, and which was provided in two different ways and

complementary.

He requests that, as mitigating circumstances, it be taken into account that he attended the

request of the interested party granting it in various formats, denying good faith in the

proposal.

TENTH: Of the actions carried out in this procedure and of the

documentation in the file, the following have been accredited:

PROVEN FACTS

1) The claimant has a holiday residence on which since 07/30/2014,

had signed a security service contract with the defendant that included installation, maintenance and operation of an alarm center.

2) The claimant states that when accessing his home, on 12/4/2015 in the afternoon, he discovered

brio, who had suffered a robbery found "the alarm center" destroyed without having been

notified, receiving a call from the Company that same morning indicating the existence

ence of connection problems.

3) The claimant exercised his right of access before the respondent on 04/07/2017 “regarding

all the information on the Securitas Direct servers related to the records and

signals sent by the alarm equipment installed on your property, as well as the copies

of the records contained in the internal memory of the alarm between the days

11/26 and 12/18/2015”. The defendant replied that the records contained in the alarm did not

fall within the category of personal data, the claimant going to the AEPD that

resolved in an appeal for reversal on 01/2/2018, to estimate the claimant's claim and indicate

when the right was provided. The defendant challenged the agreement in the contentious

civil-administrative, resolving the National Court, first section, on 07/23/2019, in

his appeal 146/2018, dismissing his claim and confirming the resolution.

4) On 03/23 and 24/2021, the claimant submits a new document to the AEPD, according to

noting that he exercised the same right before the defendant on 02/02/2021, receiving a

02/23/2021, with an Excel table that the claimant estimates that he does not meet the demand.

right.

The Excel table containing the access provided to the claimant comprises a

total of 94 log lines, plus one from a time period of 12/5/2015,

related, according to the defendant, with tests on the alarm system as part of the

facility maintenance.

The table is an elaboration of the one claimed, of what it indicates, "are data

personal”. It starts by date, not chronologically ordered and is grouped by name,

"nomenclature of the generated log" together with a description made by the defendant, "extended description of the log" that aims to inform or define what it consists of. That definition or "extended description of the log" is generic in the detail of the incident. The “generated log nomenclature” also has a general name like: “Signal informative””***COLUMN.1” or within it there are several, such as “action CRA”, which includes “communicating”, “voicemail skip”, LOCSIN. To mention Some examples:

a) "(...) external perimeter" "nomenclature of the generated log":" "Central Security priority low."

b) "Different generic actions of the Securitas human operator in the event of an incident concrete, example speech/listening enablement, call to the different listed contacts, internal comments in relation to information transmitted by contacts etcetera”- “nomenclature of the generated log”:” “CRA action”.

In some logs, it refers to "contact", without identifying or specifying which contact it refers to.

refers, as "contact does not remember the password to prove the identity and close the incidence”, or “the contacts that the Securitas operator tries to locate are not answer”, “operator gets to talk to contact”.

5) The claim gave rise to the AEPD processing the procedure for exercising the right TD/00167/2021 in which the claimed before its admission to processing and initiation, the 05/19/2021 stated that not all the logs that record the signals of the alarms, as well as the contents in its internal memory can be considered containing personal data. He states that he has prepared a report through

a law firm, signed on 01/29/2021 entitled "application of the concept of data personnel to the signals or logs generated by the alarm systems” that indicated the logs which it considers "do not imply processing of personal data, and lists the categories of the logs that it considers would be found in this assumption:

1) "Issuance of signals of a purely technical nature for communication between the devices as part of the verification protocol of their correct operation or to the record of a technical failure”. He puts as examples in his writ of appeal against the TD/00167/2021: “device battery level, network disconnection, inhibition, etc.-tera”. It was about the "Issuance of signals of a purely technical communication nature" between the devices as part of the verification protocol of their correct functioning. performance or for the recording of a technical failure”.

2) Registration of informative signals in relation to, among others, the version of the system, model or category of installed device.

3) Descriptive record of internal and technical procedures before a con-creto”. He gives as examples in his writ of appeal against the TD/00167/2021: "times waiting procedures before an event, collection and description of the event, process of capturing and making available to the operators the images or sounds, modification of internal parameters, transfer of the event to an operator, etc. He was referring to “Record description of internal and technical procedures before a specific event”.

4) Registration of technical signals in relation to the configurations of the devices. sites that do not provide information about the interested party or their habits but simply This is reflected in the calibrations of the Securitas systems for their correct operation. to.

5) Statistical information about the devices." He gives as examples in his writ of appeal against TD/00167/2021: "number of photos captured, devices activated, quality of device responses, number of disconnections, etc.).

It was referring to “Statistical information about the devices”.

In addition, it indicates:

-"these logs" could contain information on internal technical processes of the claim-

information whose disclosure to third parties could imply diffusion of trade secrets. Mencio-

For this purpose, recital 63 of the GDPR.

-The access to logs provided to the claimant excluded technical ones or those that affect third parties-

ros.

A copy of the aforementioned report was provided on 07/06/2022 in allegations to the initiation agreement

as document 1.

1) On 06/07/2021, the Director agreed to admit the procedure for processing

of “exercise of rights arts. 15 to 22”, TD/00167/2021 in which the defendant states

on 06/18/2021:

"In relation to the content of the" internal memory of the alarm installed in the home

of the claimant, it generated logs until 11/27/2021, 8:09 p.m., the time and date on which the

the intrusion into the home occurred during which said alarm system was completely

totally unused. According to the defendant, the system registered and sent capture signals

movement at 20:09 on 11/27/2015. As of that date, he could not generate more

logs of any kind. Therefore, in the time frame between 11/26 and 12/18/2015, the memorandum

Internal management could only generate logs on 11/26 and 27/2015, and there was only one generated log

to the claimant the

done in that time frame which was stated in the answer given

02/23/2021. They provide document 1, which is the table with columns of the access that was gave to the claimant on that date, which is marked in fluorescent green that log:

“11/27/2015 20:09:47/HIGH PRIORITY CENTRAL/Code generated automatically and randomly through the system for the security guard to deactivate the alarm”.

The claimant stated that he has not been given the data of the records contained in memory from the new installation of 12/5/2015 that is included in the request tion.

On 09/17/2021 the guardianship was resolved, agreeing to uphold the claim and grants a term to address the right, the decision being appealed by the defendant in replacement on 10/18/2021, resolving its dismissal on 10/27/2021, appearing electronically notified to the defendant on 10/28/2021.

2) On 12/21/2021, the defendant submitted a document in which she stated that she had sent a copy of access to the claimant, providing a written referral of 12/14/2021, in which contains a copy of the documentation that has been sent to the claimant by burofax. He The document includes the submission of the logs in "lines of code" format, which is collects in the SD systems the records and signals sent by the alarm. According to the defendant, it is the "literal transcription, in the format in which the in the SD systems of the records and signals sent by the alarm equipment.“

The claimant submitted a document on 05/07/2022 in which he considers that compliance is still not being met with what has been resolved since the defendant classifies the logs that are personal data of which they are not, it is an unintelligible picture, the expression of imprecise descriptions, the letter very small.

The table with "excel" sheets provided to the claimant, on 12/14/2021, contains the logs in chronological order of date and time and there are a total of 19 informative columns capable of containing definitions such as: "(...) of the signal", which would correspond to the tables in annex II provided by the defendant in allegations to the initiation agreement,

where its meaning is described in an extended way, not provided to the claimant, .

Fields such as description and a

more extensive description in “description (...)”, “event”, “event (...)” “Zone”,

“***COLUMN.3”, “***COLUMN.4”. “***COLUMN.1”, “time of (...)”, to name only

several with meanings and keys that were not given to the claimant.

In evidence, the defendant explained, for example, that the alphanumeric codes that

appear in the “SIGNAL” column, it is the message generated in the language itself

of the alarm system (machine language) that is translated into the information that appears

in the rest of the columns and essentially in the column of “***COLUMN.2 (...)”.

To understand the meaning of the code, you have to go to the field of this column. The system

sends messages that incorporate alphanumeric codes that are later translated

in the different columns of the log presented. The “SIGNAL” column collects the part

of the “raw” message from the system that is then translated into the rest of the columns.

To this end, the defendant explains that:

• The column “***COLUMN.2 (...)” is the translation of the system language event

so that the agent/operator understands what the message is about. This information is

complemented with the columns "***COLUMNA.1" and "***COLUMNA.2", which contain

complementary information so that the agent/operator can understand the event that

is received at the CRA.

It also appears in the personal logs provided to the claimant.

- The "ZONE" column identifies the alarm device in which the event occurs.

(eg (...), identifies a recording photosensor in programming position 2) and the

"AREA" column describes the corresponding area of the facility (eg, Home Salon)

- The column “***COLUMN.3” indicates the priority of the signal, being the values

lower priority ones.

- The column “***COLUMN.4”, contains the type of signal that represents the event (e.g.

INF is the code associated with “information”, which appears in ***COLUMN.2 (...),

SS is associated with “supervision”, as is also included in ***COLUMN.2 (...), CC is

associated with "coercion", SO is associated with "SOS", AAC is associated with "power outage", etc...).

In this way, these codes are directly linked to the information contained in the

column ***COLUMN.2 (...).”

In document 1 (REPORT of 01/29/2021, provided by the defendant in allegations),

ANNEX II offers a general analysis of the consideration as personal data of the

generic log lines that can be used in SD systems during the

development of its activity, without specific application to any interested party. The painting relates

the different “signal classes” to which the different types of logs are associated,

completed with "description", "extended description" explained by SD, "link with

the physical person" and "whether it is considered personal data or not,

However, there are 19 columns that contain keys and even descriptions.

unspecific as "information signal" that are not understandable without a

explanatory correlation.

3) In the security contract signed between the claimant and the respondent, it was stated that the

The alarm system contracted by the claimant had, among other things, photodetectors,

device that has an infrared movement sensor, a microcamera and

a flash, in case of intrusion, bypass the alarm triggered by the camera and send the notice and

the images captured to the Alarm Receiving Center (CRA), verification element

by audio, talk-listen, which is located inside the control panel and serves to

carry out audio and listening checks in the event of an alarm jump, it also serves to

talk to the customer through the switchboard or control panel

4) The basic maintenance included for the client: the remote checking services

the operation of all components (technical check according to current regulations),

updating the software and its components, with the sole purpose of providing the services

security trades.

10) In the contract, the defendant indicates that it has an image management file

and sounds that you can capture through your video surveillance systems when it occurs

an alarm jump in the homes of customers. It is added that "The CLIENT may only

have access to information on any incident or recording made as a result of

an alarm jump, sending a written request through the means that allow it in-

indicated in clause 20 of the general conditions, in which the identity of the

of the contract holder, accompanying a photocopy of their DNI, CIF, NIE or valid passport.

gor, as well as the date, time and place where the recording presumably took place”.

11) As part of the contract there is the "action plan" in which the definitions appear:

-"CLIENT: Natural/legal person who signs the CONTRACT, who is the owner of the

alarm system described in the aforementioned CONTRACT and that is the holder of the word

master key. The CLIENT may in any case have the status of user "

USER: Natural person to whom the CLIENT authorizes access to the property and the use of the

alarm system, making available the means of connection and/or disconnection of the same.

"CONTACT PERSONS: Natural person who may or may not coincide with the CLIENT of the contract and that it owns the master keyword.”

- CLIENT MASTER Password: Identifies the CLIENT and the main contacts. Has to be provided by them when they contact SECURITAS DIRECT by phone. It allows and gives access to all kinds of procedures and modifications, whether administrative (contract, action plan, etc.), or operational (verification of jumps in alarm). So that you identifies itself to Securitas")

- COACTION code: In the verification call before an alarm jump, it must be provided to SECURITAS DIRECT, by whoever is in the property in a situation of real danger to their physical and/or patrimonial integrity.

There is also a “SECURITAS PASSWORD”, “for Securitas to identify itself to you.”

They include:

-"contact list", four people identified by name and first surname, numbered, the claimant, client, with two telephones, the rest with one, all with keys.

All four are listed in another “standard action plan” listing in the chart, ordered as "contact" from 1, the claimant, to 4.

In the particular conditions, the claimant adds his email.

12) Asked the defendant in evidence about the way in which they identify themselves in the logs, the different actions of possible users in their different roles that they can assume mir: owner, authorized, contacts and in the different elements of the system, stated that

They are identified by the reproduction in the log of the interaction that may occur with each of them, clarifying that the "users with access to the system" correspond to with SD personnel who may receive a specific incident with the owner or those designated contacts and, where appropriate, carry out the operations requested by them, that give rise to logs that were considered as personal data of the claimant, to the Proceed from an action urged by him or his authorized. There are other logs that respond given to this premise as those between 12/05/2015 at 14:19:04 and 14:45:45, provided to the claimant, where ***USER.1 accesses the customer file to manage and agree on maintenance with the client associated with the event that occurred on 11/26/2015.

If the Excel table of access provided to the claimant between 05/12/2015 is examined at 14:19:04 and 14:45:45, it only shows “the operator views the low code words demand”, “event (...)” and that accesses the client's file, without indicating which owner or contact causes the request.

On 12/18/2015 at 20:08:18, as a result of a customer call to SECURITAS DIRECT in the same sense, without mentioning which owner or contact causes the petition. Appreciating that on that same day, there are logs provided to the claimant, that respond to "APP service injected event, remote disconnection connections", without that the cause of the request be correlated, outside the owner or one of the contacts authorized.

13) In addition, through an application installed on the mobile phone, users or per-Authorized contact persons can interact with the alarm system, the telephone being mobile phone a means of communication for security personnel with the claimant to whom They send SMS or emails. The defendant in evidence stated that "with the mobile device can connect or disconnect the alarm system, and that said incident is recorded in the internal memory of the device, although it is only transmitted to the CRA in case the ac-

situation responds to the existence of a security incident. In that case, it is

that is, when a security incident occurs (e.g. disconnection as a consequence of

of an alarm jump) and later the system is disconnected, the log is recorded

in the CRA identifying the user (key, command or code) that has carried out the action. Equal-

Mindfully, if the connection or disconnection is made from the App, the log is transmitted to the

CRA, reflecting that an action has taken place through an Iphone or An-

droid, but the phone number from which this action is performed is not reflected. Add

In this case, the records would be the following:

- 12/06/2015 at 1:15:27 – Disconnection. (…) 00 - User: 07 Disconnection due to jump of

alarm at 1:15:04 (...). This log records a deactivation of the alarm system by

by means of a remote control following an alarm trip.

Regarding logs associated with interactions with the alarm system through the APP,

installed on the claimant's mobile, these would be the following:

Indicates the logs started on 12/06/2015 14:06:47 Status Request from iPhone to

21:06:08 with different requests from iPhone. In the access boxes

provided to the claimant, on said date and time it is not contained or inferred that the

request is correlated with the claimant or may be through any of the contacts

authorized. In such a way that in view of the Excel table -provided access-

does not know who the person is: owner or authorized contact who requests and arms the system or

the images.

14) The control panel, also called the alarm control console, is usually located

inside the house, is the one that receives the signals from the sensors, and where
activates (arms) or deactivates (disarms), so if it is not activated (armed), it does not recognize
It will generate the signals from the sensors. The home alarm device is connected
7/365 with the CRA. The defendant reported that the connection system and the CRA are carried out
carried out using a SIM card integrated into the control panel.

The defendant stated that the control panel of the alarm system stores records
others. In fact, it can store up to ***NUMBER.3 events, which are deleted over time.
cyclically, depending on the records that are generated and recorded
continually. As new records are generated and recorded, they are deleted automatically.
cyclically the oldest ones maintaining a temporal order of recording and deletion
always within the ***NUMBER.3 records it can hold.

fifteen)

The defendant stated in evidence on the question of the way in which they are generated and
store the logs of the operation of the alarm system, which the system generates and al-
stores in the control panel records derived from:

-Customer interactions with the alarm system, for example: connection, disconnection.

-Internal verifications of the system: example coverage (...), and

-Activities of the alarm system in the performance of its function, for example, jump
alarm.

In addition, the defendant pointed out that the catalog of logs that can be generated by the
interaction of the installed system and the CRA is closed, not being possible the creation of
new logs different from those that the system generates. Some of these logs previously
configured, they will be generated as a consequence of the interaction of the system with a
activity carried out by an operator or authorized user of SECURITAS DIRECT, as well as
as well as by the owner of the system or the persons authorized by it.

The internal memory of the device is located on the motherboard of the control panel.

control. According to the defendant, said internal memory records events, among which are distinguish:

(Yo) those that generate a log, a copy of which has been provided in the document. Item No. 2 of those provided together with the pleadings to the Commencement agreement. (logs as they leave the SD system, together, those that contain data and those that do not, for chronological order).

(ii) and other merely technical events related to the interconnection produced for sending the logs to the CRA of SECURITAS DIRECT (e.g. channel through which sends the log, successful connection, acknowledgment, etc.). Since they only refer to the referral and not to any type of specific action, they consider that they would not be part of what requested by the claimant.

According to the defendant, in both cases, the destination of said records is the CRA, "although the information mentioned in point (ii) as well as the logs that do not reflect a relevant event related to the operation of the alarm do not communicate and remain in the internal memory of the switchboard and are only accessible by SECURITAS personnel DIRECT in the event of an event that requires the performance of a folaugh.

In evidence, the defendant indicated that from the CRA, the operators have the capacity to activate or deactivate the alarm only at the customer's request, within the framework of a telephone interaction with him. This request is duly registered, through its corresponding log. The assumption was given in the records provided to the claimant

on the day 12/18/2015.

16) The defendant maintains that the claimant's alarm device generated logs (re-

event records) until 20:09 on 11/27/2015, time and date on which the

the intrusion into the home and during which said alarm system was completely

useless mind. As of that date, that device could not generate any more logs.

17) In the records, there is a time jump in logs considered personal data that are

They gave the claimant between 11/27/2015 at 20:17 and 12/4/2015 at 11:05.

18) The first resumption log after 11/27/2015, (cataloged in green when considered

that contains personal data and delivered to the claimant is that of 4-12-2015, 11:05:04,

that the defendant explains that it is produced as a result of technical verifications

through an automatic system called GTI (it appears in the log itself) that is

in charge of carrying out various checks to know the technical state of the system,

proceeding to the opening of a maintenance when necessary. In this case,

an operator is in charge of calling the client to do a review with the client online

and if this is not possible, arrange a visit from a technician to verify the state of the system.

19) It can be seen that until this resumption, as well as in previous days, there are logs in

red color, no personal data, as of 11/28/2015.

20) On 12/05/2015, a new alarm device was placed at the claimant's home.

te, which replaced the destroyed one, being discharged from service on 12/23/2016.

21) Regarding whether it is possible that the logs overlap, the defendant indicated in

proves that "each log line is a unique time-stamped record, and can even there may be several in the same minute and second, as they are "machines" but this does not

it supposes an “overlay”, but rather the generation of several simultaneous logs.”

22) With the alarm on 11/27/2015, the defendant proceeded to the pertinent verification

confirmation of the same by attempting to access the system's speech/listening module. To the

not be possible, and disconnection was not received by the user, the mechanism was activated

of contact with the people and telephone numbers established in the document "PLAN OF

ACTION", informing "contact four" of what has happened up to that moment. Of is-

These facts are reflected in the logs with personal data provided to the claimant.

23) The defendant also has logs that it does not consider personal data generated

on 11/27/2015 at 20:09:47, as well as all those of the previous day, 26. The first log that was

generates the claimant as personal data is that of 11/27/2015 20:09:47. At the same time,

Two logs appear as non-personal data, in red, with different codes that

that appear in the claimant's log with a note: "intrusion seismic volumetric garage door-

panel coverage level and coverage, volumetric intrusion description radius, and the second “se-

informative signal”. There are also different red logs of the same 27 and all of the

28 to 12/4/2015, 1104:50. Between 28 and 12/4, except for 29, se-

according to the comment that appears test of Logs that report the loss of communication

with the device) up to 4, one per day.

The defendant stated that the logs of 11/27/2015, 20:09:47, begin by means of the

detection of a volumetric alarm alert at 20:09:47, generating a code

random (1155) that is generated with any alarm jump, so that if it is sent to a

watchman, he can disconnect it (in this case, it was not used to send any

vigilante, since it was determined that it was not necessary). From that moment on, there are

system verification logs for the transfer of information to an operator, who

From that moment, make the relevant calls to those who appear as contacts designated in the contract by the claimant. These attempts are unsuccessful with respect to

the first three contacts, when the voicemail is sent, being able to carry out the

communication with the room of contacts which, however, does not provide the word that

allows establishing communication, concluding the processing of the alert on 11/27/2015

at 20:17:07 hours, last log of personal data that is recorded and

delivered to the claimant.

The defendant stated that "all actions related to the alarm and

contact attempts have been considered personal data and provided to the

claimant, not having such consideration the logs exclusively related to the

the way in which the SECURITAS DIRECT systems manage and channel the

actions to be carried out in these cases or those that refer exclusively to the operator

intervener. The justifying explanation of the consideration or not of the information as

personal data is contained in the report provided as Document No. 1 in the

allegations to the Commencement Agreement.“

The defendant indicated that the logs generated from the moment the jump occurred

alarm of 11/27/2015, 8:09 p.m., and once those related to the

attempts to communicate with the contacts designated by the Complainant, refer to

successive communication attempts between SECURITAS DIRECT and the system installed in

the Claimant's address, which were unsuccessful and being machine interactions to

technical machine.

Likewise, there are different logs related to alarm jumps later deactivated on 12/5/2015 from 18:56:37, provided to the claimant by considered to incorporate personal data related to it, given that it is actions aimed at different tests on the operation of the installed system in your home, carrying out different alarm tests (volumetric, seismic, for duress or magnetic). There is also an alarm jump on 12/6/2015 at 01:15:04 hours, being able to check the logs generated by the system, and that concludes with the communication with the owner that indicates at 01:17:22 hours that the jump of the alarm may have been generated by the fireplace.

24) For the purpose of initiating the action protocol, the alarm signals are considered to be received at the Alarm Receiving Center from the capture of the elements intrusion detection, SOS button, anti-robbery button, and duress code tion. In the contract there is a protocol in this regard that distinguishes if it jumps, "without disconnecting" user connection", in which case SD verifies "by accessing the speech-listening module" system tab and/or call to the landline of the property, provided that there is the latter. If through these means:

- An answer is obtained: the person will be identified with the keyword teacher or contact If the keyword is correct, the user will be provided with the precise technical instructions for you to disconnect the system.
- If the keyword is not correct or no response is obtained: SECURITAS DIRECT proceed to comply with the verification procedures provided for in the current Private Security regulations as well as to use the complementary means verification such as proceeding to the verification call to the CONTACTS PRINCIPAL and/or OPERATORS established, and/or the Security Guard and/or F.C.S. Yeah it was a confirmed real alarm. In any case, the decision to issue the notice will correspond exclusively to SECURITAS DIRECT.

In the event that "user disconnection" occurs, it is the case in which the alarm goes off, and in less than 20 seconds (since the alarm jump), an alarm signal is received.

disconnection in the CRA. In this case, "an announcement will be automatically issued

recorded through the speech listening module of the system, in which the client will be informed

of the signal received as well as the execution of the disconnection by the user or person

authorized and the cancellation of the incident”

"In the event that the disconnection signal is received in a time greater than the

indicated in the previous paragraph, SECURITAS DIRECT will proceed to verify the jump of

alarm by accessing the system's speech-listening module and/or calling the telephone

of the property, provided that the latter is available, to carry out the

verifications that it deems appropriate according to its diligence as a Company of

Security and that are adjusted to the applicable Private Security regulations.”

The one claimed in tests, to the question of Verification mode/s of the applicable alarm/

s in this case, and which logs are generated and indicate those with this description that appear in the

period requested by the claimant, responded that they can be classified as:

(i) those that are generated as a consequence of an interaction of the holder of the contrato or an authorized by the same with the alarm system;

(ii)

those derived from a human interaction produced from the CRA; and

(iii) those that are generated automatically, without human intervention of any kind.

It considers that "only the logs listed in points (i) and (ii) imply a

processing of personal data, and of these, only the one listed in point (i) supposes the data processing of the claimant or the persons authorized by the claimant, in the

Document No. 1 (report of 01/29/2021, provided by the defendant in allegations)

provided by the defendant together with her pleadings, it was clarified that the

right of access by the interested party to their own data, only affected the

contained in the aforementioned point (i) and not to those related in points (ii) and (iii), which do not

incorporate personal data of the Claimant. "

Specifically, and with regard to all the logs contributed to the Agency, they would fit into

As described in this answer the following logs that represent verifications of

alarm:

- Logs from 11/27/2015 from 20:09:47 to 20:17:07,

moment in which an action plan is contacted. These are 21 logs in which

description they are all related to the action of the CRA, with additions such as call,

communicating, skips voicemail, leaves message on voicemail, operator gets

talk to contact 4, wrong word, or other mentions to contact 1, 2, 3, call to

H/E, H/E audio is not sent to FCS and other keys in the various frames, which as already

mentioned are not understandable without an understandable key and explanation and

Brief of its meaning.

- Logs from 12/06/2015 from 01:15:04 to 01:17:40. In the

that several logs appear, "indicates that it may be the chimney", and in the same sense with

keys in the different tables, which are not understandable without a key and explanation

understandable and brief of its meaning.

The defendant reported in evidence that, in the case of the data period requested by the

complainant, there was no confirmed alarm notification record that was

notify the Police.

25) The defendant states that "the internal memory of the switchboard (Control Panel)

initially installed and destroyed in the events that occurred on 11/27/2015, not incorporates, within the time period for which the right of access was exercised,

no log referred to (...)

being this, and no other, the reason

or off(...) of the alarm system,

for which the information provided to the Claimant does not incorporate any record of this

nature in relation to the disabled device.

Regarding the logs that were recorded in the internal memory of the system installed on the date

12/5/2015, the defendant indicates that she could not access the information at any time,

Therefore, it was not possible for him to provide it to the interested party. As for the reason, he points out that

the CRA, can only access the logs that are transmitted to it from the

internal memory of the device, but not those of a merely technical nature that are

generated in said internal memory, since SECURITAS DIRECT can only

access the content of said device in the event of a

incident requiring forensic analysis. In this case, given that said incident had no

Instead, the device remained in the Claimant's home until the end of the

Contract, without at any time SECURITAS DIRECT being able to access said

internal memory nor was it necessary to carry out any forensic analysis of its

content, in the absence of an incident that required it. how can

verified, these answers do contain information referring to the period

mentioned in the question posed.

26)

The defendant stated in evidence that after accessing the records contained in the memory of the alarm, it has been verified that it was connected from the day 11/22/2015 at 11:56 and that it did not present any anomaly.

27) Regarding access to personal data contained in the internal memory of the panel of control, after the placement of the new one on 5/12/2015, do not appear in the access provided from 12/14/2021 nor in the precedent of 02/23/2021.

28) In document 2 of allegations, -total logs- Excel table of all logs, differentiated in red-considered as non-personal data by the defendant-, and in green, considered as personal data by the defendant, figure yes:

With different keys of the "(...) of the event" distinguished in red those considered non-data personal, example, there are two in red, from 11/27/2016 20:09:47, and another with the same date and time, in green. The defendant stated that the logs refer to different events: the first it involves the detection of an alarm jump detected by a volumetric sensor; the second involves the generation of a deactivation code in case it is necessary to go to the house once the corresponding verifications have been carried out, which they also appear in the log table; and the third refers to coverage (...).” Add that dates and times can also coincide in the logs that have personal data, providing the example of 12/5/2015 18:38:10 in which there are five different, related with on-site maintenance of alarm change.

29) The defendant reported in evidence that the periodic reviews of the fund system operation of alarms provided for in article 43 of RD 2364/1994 approving under the Private Security Regulations and article 5 of Order INT/316/2011, are carried out from your CRA remotely, normally every three months. In addition, rea-

Conducts daily communication tests and correct transmission of the alarm system with the CRA automatically. Give some examples from 5/12/2015 that are included in the logs provided to the claimant and from 12/6/2015, 18:45:42, which is not considered a log of

Personal data of the claimant, appearing in red.

On-site reviews are recorded in the log of the management system of the

CRA alarms, since the technician must check a series of parameters of the

system and carrying out the various functional checks.

If remote reviews were carried out, these would be reflected in the event memory

of the alarm system.

On the other hand, maintenance tasks are corrective, aimed at resolving

specific incidents that do not allow the proper functioning of the system of the

alarm, and are intended to rectify said incidents, and may be carried out

according to the nature or need, in person or remotely.

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR) recognizes each

Control Authority, and as established in articles 47, 48.1, 64.2 and 68.1 of the

LOPDGDD, is competent to initiate and resolve this procedure the Director of the

Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

processed by the Spanish Data Protection Agency will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations dictated in its development and, insofar as they do not contradict them, with character subsidiary, by the general rules on administrative procedures."

II

Article 4 of the GDPR, under the heading "Definitions", provides the following:

1) “personal data: any information about an identified natural person or

identifiable (“the data subject”); An identifiable natural person shall be considered any person

whose identity can be determined, directly or indirectly, in particular by means of a

identifier, such as a name, an identification number, data of

location, an online identifier or one or more elements of identity

physical, physiological, genetic, mental, economic, cultural or social of said person;”

"7) "responsible for the treatment" or "responsible": the natural or legal person, authority

public authority, service or other body that, alone or jointly with others, determines the purposes and

means of treatment; if the law of the Union or of the Member States determines

the purposes and means of the treatment, the person in charge of the treatment or the criteria

for their appointment may be established by the Law of the Union or of the

Member states"

In the present case, in accordance with the provisions of article 4.1 of the GDPR, the

processing of personal data, since SECURITAS DIRECT

carries out, among other treatments, the collection, conservation, consultation, use, access

of the personal data of the clients-users, such as: name, surname, email

electronics, credentials…, etc.

SECURITAS DIRECT carries out this activity in its capacity as the person responsible for the

treatment, since it is who determines the purposes and means of such activity, by virtue of the

article 4.7 of the GDPR.

This disciplinary procedure is initiated because the complaining party considers

that their right of access derived from TD/00167/2021 has not been met, alleging

that not all your personal data (logs) have been provided and that those that have been sent are unintelligible to you, in the terms established in the background of this resolution proposal.

Thus, in this sanctioning procedure, it is a question of elucidating, through the instruction of the itself and taking into account the allegations and documentation provided by the claimed party, whether the right of access has been fully met, and how it has been carried out carried out, in the terms established in the GDPR, and, therefore, if there has been an infringement of the data protection regulations.

II

As highlighted in the Statement of Motives of Law 5/2014, of 4/04, on Private Security vada, security is one of the fundamental pillars of society, it is found in the basis of freedom and equality and contributes to the full development of individuals. Bliss law considers private security as an activity with its own entity, but at the same time as an integral part of public security.

The activity of operating a security system through a CRA is that exclusive, complementary service or activity of a commercial nature and prevention of crime, subordinated to public security, developed and provided by companies of Security approved by the Ministry of the Interior, subject to the regulations of Private security, which use means, technical measures, protection elements, regulated and approved, through electronic security systems against risks of theft or intrusion with the functional characteristics described in the Standards UNE for its commercialization, sale, installation in a private area demanding

Private security. This is materialized through the signing of a contract of leasing of maintenance services and connection of said system to a Center Control integrated in the Alarm Center also authorized, for the reception, treatment, verification of alarm signals emitted by said security systems installed, through the technical and human procedures provided for in the Order 316/2011 of 1/02 on the operation of alarm systems in the field of private security, in such a way that its reality can be determined or not, and its communication in case of being confirmed as real to the Police.

The purpose of this contract is the provision or material delivery by the Company of Security of a Security System and its installation with a service purpose of Alarm Receiving Center, and later the maintenance of the system in proper functioning for the provision of contracted services at home (home) of the contracting user.

Upon finding the installation of the device and security elements linked to the maintenance of the same as a system or product that is linked to a service of exploitation through an alarm receiving center, it is a contract of service linked to the maintenance service of the installed system, dedicated exclusively for reception of alarm signals emitted by the security system installed and to the treatment of said signals for the determination of their real origin or false by complying with established regulatory procedures.

The mentioned order of operation of the alarm systems establishes that the CRA I carried out verifications through rules contained in technical procedures described and complementarily human. After completing these formal requirements and materials required, said alarm signal confirmed by the CRA can be communicated

as real to the Police.

The judgment of the Provincial Court of Madrid, section 11, 98/2014, of 03/11/2014,

analyzes the nature of the security contract in its mode of provision of

central alarm services by a company dedicated to it, indicating in its

second legal basis:

“As this same Chamber already stated in its Judgment of June 30, 2011,

which refers to the one of April 29, 2010, which in turn refers to the one issued on

June 2007, citing the Judgment of the A.P. of Barcelona of December 30, 2004,

"...the contract signed by the parties is a service lease contract and not a

work, and this based on doctrinal criteria accepted in the jurisprudence of the Court

Supreme Court (S. 4.2.1950, among others), which are supported to establish the difference, in the

immediate object of the lease obligation, so that if the lease agrees to the

provision of a service or work of an activity itself, not the result that

that provision produces, which is the case at hand, the lease is of

service. And on the other hand, if the provision of a result is obligated, without considering the

work that creates it, the lease is work. Well, the obligation of the

defendant, appealed today, is an obligation of activity, and not of results.

It is evident that the purpose of the contract was to provide the commercial premises with

security measures aimed at preventing the commission of criminal acts and the

Defendant's fundamental obligation was to provide the services necessary for the

the installed security mechanisms work correctly.

Pursuant to the security services lease contract, the entity

defendant, undertook, not to avoid the possible commission of robberies in the farm, nor to ensure in any case the restitution (in kind or in cash equivalent) of what third parties could steal, but exclusively to respond as normal operation of a security system, consisting of a burglar alarm with telephone connection with the alarm center, making the detection by sensors located at various points throughout the offices, so that the system had to transmit -via telephone- a signal to the Alarm Center, which in turn had to give notice of the possible crime to the security forces, so that they prevent their consummation, therefore, had an essentially preventive and protective purpose, therefore, as has been exposed, the object is in the activity, and in these terms, they are the only possible to demand responsibility".

The sending and receiving of signals by the device and the CRA occurs in a home particular, understanding as such, a suitable space to develop private life in it, on which its inviolable nature will affect, as provided for by the EC in its article 18.2 infringement that can occur regardless of whether, at the time of the entry, whether the holder of the right is inside or outside his domicile. In addition, there is a close relationship between the inviolability of the home and the right to privacy enshrined in art. 18.1, as STC 22/1984 rightly pointed out, "the inviolable domicile is a space in which the individual lives without necessarily being subject to the uses and social conventions and exercises his most intimate freedom".

The inviolability of the home therefore guarantees that intimate sphere of personal privacy and family (within the limited space that the person himself chooses), in front of all kinds of invasions or attacks by other people or public authorities not consented to by

the right holder. The constitutional protection of the domicile thus has an institutional character.

instrumental.

IV.

The defendant provided some details about the operation and components of a

alarm system.

Basically, a control panel is installed at home, which is usually accompanied by

an alarm kit (additional items such as motion detectors/camera and that

may allow viewing via a mobile device connected via a

installed application, together with other means such as remote control, sirens, reader of

keys, smart keys that allow the alarm to be disconnected simply by bringing the

key to reader, magnetic detectors etc.)

The control panel that is usually installed inside the home, in a place that is not

be very visible, it is connected to the CRA, where notifications and warnings arrive

like alarm jumps.

In turn, the CRA must carry out operations to verify and analyze the anomalies that

can occur, control of power outages, alarm triggering for different

Reasons to give some examples. At the same time, in remote mode, the ARC can

activate, configure and verify the functions of the alarm system, perform diagnostics of

connection, and control the alarm detectors.

The control panel allows to activate the system, arm, disarm the alarm, connects with the

additional elements such as sensors and receives signals from detectors

installed peripherals. For example:

-if a door contact or a movement sensor is activated, the panel will give the signal, if

the alarm is not deactivated with a valid user code, the system assumes that there is a

intrusion and will give an audible or light signal, at the same time as communicating with the CRA.

-If the panic, SOS or anti-robbery button is activated, it directly communicates with the CRA

It also allows bidirectional communication with the CRA via microphone and speaker.

integrated (listening speech module).

The CRA is in charge of analyzing and interpreting the alarm jumps, it is the headquarters of control of alarm systems.

When the alarm jump is attended, the CRA has to analyze the information thoroughly to determine what type of emergency it is or if it is a false alarm.

In any case, the CRA will contact the owner or contacts designated to inform you of what happened.

The communication between the control panel and the CRA can occur by various means and method. In general, the communication between the alarm systems and the CRA, is given through two different communication paths to allow communication is continuous, even if one of the ways fails or is sabotaged.

Bidirectional communication with the alarm system is allowed from the CRA, being able to access the system through the software for remote control of the system, this also regardless of whether the system has lost mains power installation.

Systems in general, record the activity of authorized users (customer and contact persons designated by him), as well as operators of the claimed, including machine-to-machine operations generating access traces: -log in-, origin, uptime, actions, and connections.

The information in these records is essential for preparing management reports and for monitoring. Among the events that the different systems record, are for example the start, end of session, access, modification of files and directories, change in the main configurations, program launches, etc.

The activity records of the different systems and equipment are the data from the which it is possible not only to detect performance failures or malfunctions, but also detect errors and intrusions. With them, systems of monitoring that properly configured can generate alerts in time real. On the other hand, they facilitate forensic analysis for the diagnosis of the causes that cause the incidents. Finally, they are necessary to verify compliance with certain legal or contractual requirements during audits.

V

Putting things this way, the claimed party considers that the "technical" or "internal", are not personal data of the complaining party, not having, for therefore, obligation to provide said data as part of the right of access exercised by the latter.

The question excepted by the claimed regarding the data of personal nature of those named by the defendant: “technical” or “internal” logs, which are characterized, as he defends, by not referring to any person, specifically or even the claimant and for not containing information about any person, or even the claimant. Adding also that it considers them confidential, worthy of the protection of business secrets.

It must be based on article 1 of the RGPD in which it is established as an object

"1. This Regulation establishes the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of such data.

2. This Regulation protects the fundamental rights and freedoms of

natural persons and, in particular, their right to the protection of personal data.

The exercise of the right of access is carried out both within the framework of the legislation in

data protection, in accordance with the objectives of the legislation in

data protection, such as, more specifically, in the framework of the "rights

and fundamental freedoms of natural persons” and, in particular, their right to “the

protection of personal data”, as established in article 1, paragraph 2, of the

GDPR.

It is essential to understand that it is about determining how to apply the

provisions to certain situations in which individual rights are at stake

game for the processing of your personal data.

Article 8.1 of the Charter of Fundamental Rights of the European Union states: “1.

Everyone has the right to the protection of personal data that

concern.

Recital (26) indicates: "The principles of data protection must be applied to

all information relating to an identified or identifiable natural person. The data

pseudonymous personal data, which could be attributed to a natural person through the

use of additional information, should be considered information about a person

identifiable physics. In order to determine if a natural person is identifiable, the

into account all means, such as singling out, that you can reasonably use the data controller or any other person to directly or indirectly to the natural person. To determine whether there is a reasonable probability that means are used to identify a natural person, must be taken into account all objective factors, such as costs and time required for identification, taking into account both the technology available at the time of treatment and the technological advances. Therefore the principles of data protection should not apply to anonymous information, that is, information that is not related to a identified or identifiable natural person, nor to the data converted into anonymous of so that the interested party is not identifiable, or ceases to be. Consequently, the This Regulation does not affect the treatment of said anonymous information, including for statistical or research purposes."

Opinion 4/2007 of the Article 29 Working Group on the concept of data personal, indicates that it is: all information about an identified physical person or identifiable.

The definition reflects the intention of the legislator to maintain a broad concept of "data personal", which requires a broad interpretation that includes all information that can be linked to a person, or refer to an identifiable person, in order to to protect the freedoms and fundamental rights of natural persons, among others, particularly your right to privacy in regards to data processing personal.

This breadth in terms of the extension of the term "personal data", such as the diversity of fields in which it can be manifested, is confirmed in various judgments of the CJUE, by way of example in that of 12/20/2017, case C-434/16, paragraphs 33 to 35:

"33. As the Court of Justice has already pointed out, the scope of application of the Directive 95/46 is very broad, and the personal data to which it refers are heterogeneous (judgment of May 7, 2009, Rijkeboer, C-553/07, EU:C:2009:293,

paragraph 59 and cited jurisprudence).

34 Indeed, the use of the expression "all information" in the definition of the concept of "personal data", which appears in Article 2(a) of the Directive 95/46, evidences the objective of the Union legislator to attribute to this concept a very broad meaning, which is not limited to confidential data or data related to the privacy, but can cover all kinds of information, both objective and subjective, in the form of opinions or appreciations, as long as they are "about" the person in question.

35 This last requirement is met when, due to its content, purpose or effects, the information is related to a specific person...” (The underlining is ours).

The doctrine elaborated by the CJEU regarding the breadth with which the concept of personal data has been adapted, taking into account the various advances technological. Thus, in the judgment of 11/24/2011, case C-70/10, in its paragraph 51 considered that IP addresses are protected data of a personal nature, since that make it possible to specifically identify such users. This criterion is maintained and extends to the cases in which it is even dynamic IP addresses, those temporarily assigned by network access providers to their clients, considering that they continued to constitute personal data when the person in charge to store them, in this case the owner of a website, did not have the data necessary for the identification of the specific user, but that they were in possession of a third party, picking up this criterion, again favorable to an interpretation of the concept of personal data, in the STJUE of 10/19/2016, in case C-582/14, Patrick Breyer and Bundesrepublik Deutschland, when asserting that IP is data of a personal nature for the service provider: "article 2, letter a), of the Directive 95/46 must be interpreted in the sense that a dynamic IP address recorded by an online media service provider on the occasion of the query by a person from an Internet site that that provider makes accessible to the public constitutes personal data with respect to said provider, within the meaning of the aforementioned provision, when he has the legal means that allow him to identify the person concerned thanks to the additional information available to the service provider Internet access of said person” (paragraph 49).

More recently, in its judgment of 06/17/2021 (Case C-597/19), analyzing a load assumption, from the terminal equipment of a user of a network between peers (peer-to-peer) and towards the equipment of other users of said network, of parts, previously downloaded by the aforementioned user, from a multimedia file that contains a work protected, even if those parts are only usable by themselves from a certain download volume and in which it is the software itself that automatically gives rise to the aforementioned charge, in its paragraph 97 it recalls that "With preliminary nature, it is necessary to point out that in the main matter there are two different personal data processing; namely, one that you already initially performed Media Protector on behalf of Mircom, in the context of peer-to-peer networks.

peer), consisting of registering the IP addresses of users whose peer connections The Internet was supposedly used, at one point, to upload works protected in the aforementioned networks, and another that, according to Mircom, should be carried out by Telenet in a later phase, consisting, on the one hand, of identifying those users by comparing the aforementioned IP addresses with which, at that very moment, Telenet had assigned to the aforementioned users to carry out said charge and, on the other hand, to notify

Mircom the names and addresses of those same users”.

In light of the broad scope of the definition of personal data, a restrictive assessment

of such a definition by the data controller would lead to a

misdetermination of what is personal data and, ultimately, to a

violation of the contents by the RGPD to the interested parties, among which is the

Right of access.

The AEPD, as part of its function of supervising the application of the legislation on

data protection, must interpret the exceptions to the application of the concept of

personal data such as the one defended by the defendant, since if her theory were validated

on a part the logs of the alarm system, perhaps they would be outside the scope of

application of the GDPR.

The aforementioned breadth in the definition of personal data is defined by:

-"all information", including all data that provides information,

whatever the class of this that is to have a broad interpretation, encompassing

subjective or objective information, including evaluations, diagnoses or opinions.

-“about” a natural person, thus relating any type of information about a

Physical person. Here it is essential to connect the purpose of the information with the

"on" whom it is treated and the effects it may have for that person.

-"identified" or "identifiable". Refers to any person whose identity can be determined,

directly or indirectly, in the sense that, to qualify data information personal, it is not necessary that such information by itself allow the identification of the

interested. In this case, the information that makes it identifiable are the logs, which both

the so-called technicians by the defendant, such as those considered to be personal data

claimant's staff, appear in relation to a device, structured in a single and

unitary compact block set chronologically ordered to reflect the

events from the device referred to said claimant that is identifiable.

Opinion 4/2007 adds: "In cases where, at first sight, the identifiers

available do not make it possible to single out a specific person, this person can still be

"identifiable", because that information combined with other data (whether the

responsible for their treatment is aware of them as if not) will allow to distinguish

to that person from others". In this case, not everyone can identify you, but the

Securitas personnel yes, and if there is someone who can do it, it would be enough,

-regardless of the content or nature of the origin of the information.

-As the defendant has already reproduced in his report of 01/29/2021, provided by the

claimed in allegations, regarding information "about" a person, the Opinion

4/2007, exemplifies its meaning with: "the data included in the personal file of a

person saved in the personnel department of your company, who are

clearly related to your status as an employee of said company. But not

It is always so obvious to establish that the information is "about" a person

concrete. On some occasions, the information provided by the data refers not to

both people and objects. These objects usually belong to someone, or can be under the influence of a person or their authorized, or exert an influence on it or may have a certain physical or geographical proximity to persons or other objects. In such cases, the information can only be considered indirectly refers to those people or objects. A similar analysis can be applied when the data refer in the first instance to processes or events, such as the operation of a machine when human intervention is necessary. Low

In certain circumstances, this information may also be considered information "about" a person.

- "We are before a third category of «envelope» when there is an element of "result". Despite the absence of an element of "content" or "purpose" data can be considered to be "about" a particular person because, taking into account all the circumstances surrounding the specific case, it is likely that its use affects the rights and interests of a certain person. Enough with that the person may be treated differently by other people as consequence of the processing of such data."

It should be noted that the scope of the concept of personal data and, therefore, the differentiation between personal data and other data, would form an integral part of the evaluation carried out by the data controller to determine the scope of the data to which the interested party has the right to obtain access, elements that would be to include in the "privacy by design" configuration. In this case, the

The defendant indicates that it was not until 2020, when it began to analyze the treatment of the logs, of the alarm devices connected to the CRA, serving the report of 01/29/2021 also as a management tool, of the requests to exercise rights.

In this case, it is the installation of an alarm, a device that controls 24 hours a day, every day of the year, the security of the housing in a private address, which is implemented through a security contract and

that has a device installed in the claimant's home connected with elements

additional verification, and that, for its correct functioning, it also requires

maintenance and monitoring, and must be connected. From system settings

It is correlated that, from its use, interactions and alarm jumps, logs are generated that are

correspond unequivocally with personal data of identified persons,

identifiable and information about each other, those identified and those who

may be identifiable.

Focusing on the refusal of the defendant to classify as logs that are data from

of a personal nature, to the so-called technical logs, that is, because they do not collect information

about an interested party, nor does it pretend to know information, and their

rights and freedoms, it must be remembered that these logs that are discarded from the scope of

application of the GDPR, the claimed party classifies them into categories, which would consist of

briefly, in:

-technical communication signals between devices in order to verify the correct

operation or failure records.

-gather information through informative signs,

-Internal records before a specific event.

It is observed in the report of 01/29/2021, provided by the defendant in allegations, in the

Table I, which appear as descriptions of this type of technical logs, and which are

would therefore find in one of the three categories explained above, assumptions

such as: "information on alarm jumps", "alarm jump on sensors", or
“periods in which there is a loss of connection between SD servers and the
device installed in the home of the interested party", the "cancellation of the incident",
“relevant signal that is transmitted to an operator to start the management process”,
”issuance of periodic technical signals to confirm that it is indeed
connection and willingness to carry out the activity”. All of them, according to the defendant, respond to
internal communication-verification protocols, without explaining how it considers that these
logs, both for their content and for their effects, does not estimate that they can affect the
rights and interests of the interested party or how he considers that they are not referred to him, if,
In addition, when extracting them from the system they appear grouped and related to the person in the
claimant and his home to use them for the purposes of security control of events and
correct functioning of the system, and that would constitute information that concerns you.
The consideration of personal data that "concerns" you should not be interpreted
way too restrictive. This is how Directives 1/2022 interpret it, on the
rights of the interested parties, right of access, version 1.0, adopted on 01/18/2022,
by the European Committee for Data Protection and that appears on its website, although in consultation
public from 01/28 to 03/11/2022. In its numeral 103, it indicates that "the classification of the
data such as personal data relating to the data subject does not depend on the fact that such
personal data also refer to another person. Therefore, it is possible that the
personal data refers to more than one person at the same time and in its numeral
104, that "The words "personal data concerning you" should not be interpreted
in an "overly restrictive" manner by data controllers, as already
declared the Working Group of Article 29 in relation to the right to portability of
the data. Transposed to the right of access, the CEPD considers, for example, that the
recordings of telephone conversations (and their transcription) between the interested party
included in the right of access, provided that the latter are data

personal”.

The aforementioned Directive 4/2007 establishes, as already mentioned, that: "in some

Sometimes, the information provided by the data refers not so much to people

like objects. Those objects usually belong to someone or are under the influence of

a person or exert an influence on it”, and that in those cases, there is the

possibility that the information refers to those people, albeit indirectly.

Well, in the case that we are examining, all the logs, including those

generated and stored in which the owner-users do not intervene, is operated by

SD employees in processes in which the owner does not interact, be it in operations

internal techniques that reveal information about the effectiveness and operation, by

be the alarm installed in your home, linked to the contract for the provision of

subscribed services, establish a connection between the object (the alarm) and the affected,

since the alarm is identified with a unique identifier (a numbering

specific for each alarm device) for that service that inevitably links

the interested party with the device and everything that is generated and recorded in relation to the

same. If we take any of the submitted logs in isolation, they would identify the

that person.

According to SAN 3091/2019, of July 23, 2019, "On the one hand, it is a

natural person, and therefore fully identifiable, who signs an installation contract and

maintenance of an alarm for the protection of your home with the company

actor security. Signature of the contract from which a series of rights regarding custody and security of said home. On the other hand, and this It is important to highlight it, the right of access is exercised with respect to records and signals captured and sent by the alarm equipment installed in a private home, being exercised precisely by the person who owns said domicile.”

Thus, in this case, with this link between the alarm and the interested party, through the unique identifier that links the alarm to the contract and to the interested party, alarm system that put into operation or programmed, generates information about that person, so that all the logs discussed are considered personal data.

Apart from the fact that the information may relate directly to the claimant, for be identified or be able to be identifiable as it is in active interactions or passive, it is also identified indirectly because the information of the logs, all, including the technicians, associated with the object or device, which would indicate that the information will be about the claimant because they are affected by their right to security of your own home and in your own home, affecting those logs.

Both the technical logs named after the defendant, as well as the rest, remain stored and guarded by the defendant, document and contain information directly or indirectly on the safe operation of your contracted system, is its object, as regards the claimant or concerns him, at least. His interpretation does not would be complete if it is considered to separate this information that the defendant calls "technical logs" that he considers should not remain but stored in his possession, without that have to be used as an instrument provided to the claimant for his knowledge.

In addition, all logs and event records, both the so-called technical by the claimed party as well as those that are not, are included in the same "raw" or "online" format, because they appear interrelated and conditioned, so chronologically, with the difficulty of its understanding if not completely, and advising their protection in terms of integrity in their security jointly.

It should not be forgotten that one of the functions of the logs can be to avoid the modifications or their follow-up to know the events. On the other hand, for For example, an access due to a security breach would obtain full information by appear ordered according to a single purpose. On the other hand, that the software used or its options configure the logs as "technical" cannot be used to extend the total and automatic exclusion of the entire log, but exclusive and exceptionally, of the data that, based on the descriptive or key qualities that hold, have a substantial impact on the trade secret.

Consider, for example, the technical logs collected on the day of the intrusion and the

subsequent days, which relate to internal operations for which the defendant can deduce what happened, and the consequences drawn from the connection of the days later, days of lack of connection, all of them affect the right of the claimant because they are related to the right to security of their goods and property that the tries to protect by permanent operation of the device and warranty by signing a contract with obligations and rights for both parties.

In this way, only the defendant could understand what happened to the system contracted by the claimant, when the technical logs, which are linked to the person of the claimant, are also considered to affect directly or not the claimant's rights. In addition, it must be added that in the face of the same events, events that occurred at the same moments, such as alarm jumps, or power cuts, that other type of logs are generated that the defendant considers must be have a differentiated treatment for being technical.

In short, the processing of log data is for the purpose of executing the security contract, resulting in one of its objects being the log record, which are all related to home security. The relationship between the system, signals and owner of the alarm system given the purpose of the treatment of the logs and the object on which it falls is evident, since the technical logs that identify the claimant also concern his right that he holds as owner and responsible for the correct use of the contracted system, in front of which said registration of events, fundamental means for the affected right of the claimant.

These log record data, which in this case the defendant denies are of a personnel, defining them as technicians, grouped by responding to internal protocols of communication-verification, registration of signals or internal procedures, can actually be used for example also for forensic purposes in a case of responsibility for the operation of the system of which the owner is the claimant.

Undoubtedly, the system with all its records is identified with the claimant, affecting their rights and interests. It cannot be deduced that these data are not information about an identified or identifiable person and also part of their rights affected, such as the theft suffered, are related to the logs, including those that the defendant considers technical and that actually identify the claimant and directly affect their rights.

In conclusion:

1. The GDPR determines what personal data is in its article 4: “data personal: any information about an identified or identifiable natural person ("the interested"); An identifiable natural person shall be considered any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, a

online identifier or one or several elements of physical, physiological,

genetic, psychological, economic, cultural or social of said person;”

2. The complaining party has entered into a security contract with the complaining party. For

For this, an alarm device is installed at the home of the claimant.

3. The alarm device located in the claimant's home is identified with a

unique and permanent identifier (a specific numbering for each device of

alarm) for that specific contract for the provision of services.

4. Through the alarm system, logs linked to the alarm device are generated

installed in the domicile of the complaining party, attached in turn to the contract signed by

the latter with Securitas Direct. The SAN 3091/2019, of July 23, 2019, defines the

logs as "records and signals captured and sent by the alarm equipment installed in

a private residence."

5. Each one of the logs without distinction inevitably links, therefore, the interested party with

the device, with everything that is generated and recorded in relation to it, and with the

signed contract. Each of the logs uniquely identifies the interested party.

6. In addition, all logs concern the interested party in relation to his rights, since

that the logs are connected to the security of the home, affecting the

claimant regarding his right to the safety of his home and security in his

own home.

7. The logs identify the claimant, as it is information about a natural person

identified.

Therefore, in this specific case and considering the context, and having examined all the concurrent circumstances, the access content must include all logs generated by the alarm system, including what the claimed party calls as “technical” logs, as they are considered personal data under the terms of the Article 4 of the GDPR, including those that have not been delivered because they are classified as technicians for the claimant.

It is concluded, in this specific case, that all the logs are personal data, including those called technicians by the defendant, who identify the claimant and affect the claimant in one way or another, so they would enter into the right of access that should be provided.

SAW

Regarding the statement by the defendant that the "logs that do not imply treatment- data processing”, that is, the “technical” logs, could contain information about procedures internal technical data, whose disclosure to third parties would imply the assignment to third parties of your "know how" or trade secrets, recital 63 of the GDPR states:

Interested parties must have the right to access the personal data collected that concerned and to exercise that right with ease and at reasonable intervals, in order to know and verify the legality of the treatment. This includes the right of data subjects to access data related to health, for example the data of your medical records that contain information such as diagnoses, test results, evaluations of physicians and any treatments or interventions performed. all interested must, therefore, have the right to know and to be communicated, in particular, the purposes for which the personal data is processed, its processing period, its recipients, the implicit logic in any automatic processing of personal data and, therefore, at least when it is based on profiling, the consequences of said treatment. If possible, the data controller should be empowered to provide remote access to a secure system that offers the interested party direct access to your personal information. This right must not adversely affect the rights and liberties of third parties, including trade secrets or intellectual property and, in In particular, intellectual property rights that protect computer programs. No However, these considerations must not result in a refusal to provide all the information to the interested party. If you process a large amount of information relating to the data subject, the data controller should be empowered to request that, before If the information is provided, the interested party specifies the information or activities of treatment referred to in the request.” (The underlining is ours).

Reference is made to the limits in terms of the modality of obtaining the right of access that It is contained in article 15.3 and 4 of the GDPR, which indicates:

"3. The person responsible for the treatment will provide a copy of the personal data object of treatment...

4. The right to obtain a copy mentioned in section 3 will not negatively affect the rights and liberties of others.”

Thus, the right to obtain a copy regarding the right of access "must not infringe the rights or freedoms of third parties, including business or proprietary secrecy intellectual property, including copyright protection software. However, it reiterates, these considerations should not lead to the denial of all information to the interested party

Directive (EU) 2016/943 of the European Parliament and of the Council of 06/08/2016 on to the protection of undisclosed know-how and business information

(trade secrets) against their unlawful collection, use and disclosure, which has been

transposed into our legal system by the Business Secrets Law 1/2019 of

02/20, indicates in its recitals 34 and 35:

“(34) This Directive respects fundamental rights and observes the principles

recognized, in particular, in the Charter, especially the right to respect for private life.

da and familiar, the right to the protection of personal data, the freedom of

expression and information, professional freedom and the right to work, freedom of

company, the right to property, the right to good administration, in particular

access to the files, while respecting the commercial secret, the de-

right to effective judicial protection and an impartial judge and the right to defense.

(35) It is important that the right to respect for private and family life and to

the protection of personal data of any person whose personal data may

be processed by the holder of a trade secret when steps are taken for the

protection of trade secrets, or of any person involved in a legal proceeding related to

against the unlawful acquisition, use or disclosure of trade secrets, in accordance with

this Directive, and whose personal data are processed. Directive

95/46/CE of the European Parliament and of the Council regulates the processing of personal data

procedures carried out in the Member States in the context of this Directive and under

the supervision of the competent authorities of the Member States, in particular the

independent public authorities designated by them. Therefore, this Directive

should not affect the rights and obligations provided for in Directive 95/46/EC, in particular the rights of the interested party to access those of their personal data that are subject to treatment and to obtain the rectification, deletion or blocking of the data due to its incomplete or inaccurate nature and, where appropriate, the obligation to process the data of a sensitive nature in accordance with article 8, paragraph 5, of the same Directive goes."

A similar limitation to that provided for in article 15.4 of the GDPR applies to the right to portability that is developed in article 20 of the GDPR, establishing its number 4 that "The right mentioned in paragraph 1 shall not adversely affect the rights and freedoms of others". Bearing in mind that the right of access to the copy, such as the right to data portability are among the components fundamentals of the GDPR, the reasoning that for this limitation indicated by Working Group 29 in the guidelines on the right to data portability, adopted on 12/13/2016 determine that: "It can be understood, although they are not directly related to portability, that mention includes also "commercial secrets or intellectual property and, in particular, the rights intellectual property rights that protect computer programs. However, although These rights must be taken into consideration before responding to a request for data portability, "these considerations should not result in the refusal to provide all the information to the interested party".

As a conclusion to the allegations of the defendant, considering the right of access of the interested party and the rights of the claimed party, attention must be paid to the conciliation of rights of both parties in accordance with paragraph 4 of article 15 of the GDPR in the execution the execution of part of the content of the copy of the logs that make up the de-
right of access

In this way, the condition provided for in article 15.4 of the GDPR would be restricted not to the copy of the logs, which are all the logs as it has been motivated, but to the part of the copy of log data that may denote information affected by the trade secret in the terms Minos that in the following foundation of law we will explain.

VII

Any person enjoys, by virtue of article 15 of the GDPR, the right of access to the personal data that concern you and are subject to treatment, which establishes:

"1. The interested party shall have the right to obtain confirmation from the data controller of whether or not personal data concerning you are being processed and, in such a case, right of access to personal data…”

"3. The person responsible for the treatment will provide a copy of the personal data object of treatment. The person in charge may receive for any other copy requested by the interested party a reasonable fee based on administrative costs. when the The interested party submits the application by electronic means, and unless he requests that otherwise provided, the information will be provided in a user-friendly electronic format. common.

4. The right to obtain a copy mentioned in section 3 will not negatively affect the rights and liberties of others.”

The right of access called habeas data or "habeas scriptum" constitutes the core essential of the right regulated in art.18.4 of the Constitution -STC 292/2000 and consists in which the affected party can demand that the person in charge make a provision. The scope of the right of access is determined by the scope of the concept of personal data defined in article 4, paragraph 1, of the GDPR.

The right of access should not be considered in isolation, as it is closely related to other provisions of the GDPR, in particular the principles of data protection, including fairness and lawfulness of processing, the obligation to transparency of the data controller and other rights of the interested parties provided for in chapter III of the GDPR. Special importance in this procedure Articles 5.1 b) to d), which recall:

1. Personal data will be:

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

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which are processed ("data minimization");

d) accurate and, if necessary, up-to-date; all measures will be taken

Reasonable reasons to delete or rectify without delay the personal data that is inaccurate with respect to the purposes for which they are processed ("accuracy");

The protection of the fundamental right to the respect of Data Protection of character

This implies, in particular, that any natural person can ensure that the data information about you are accurate and used lawfully. The aforementioned right of access may be essential, in particular, to enable the data subject to obtain, in where appropriate, of the data controller, a rectification, deletion or the blocking of such data and, consequently, exercise other rights that are related to the purposes for which they were collected.

In this sense, although alluding to the then current Directive 95/46 of Parliament

European Union and of the Council, of 24/10/1995, regarding the protection of natural persons in

with regard to the processing of personal data and the free movement of such data,

The Court of Justice of the European Union ruled in the "Rijkeboer" case,

C/553/07, of 05/07/2009:

51“The aforementioned right of access is essential for the interested party to be able to exercise

the rights provided for in Article 12(b) and (c) of the Directive, namely,

In your case, when the treatment does not conform to the provisions of the same, obtain

of the data controller, rectification, deletion or blocking

of the data [letter b)], or that proceeds to notify the third parties to whom

communicated the data, any rectification, deletion or blocking carried out, if it is not

impossible or involves a disproportionate effort [letter c)].

52 The right of access is also a necessary condition for the exercise by the

interested party of the right to oppose the processing of their personal data, contemplated

in Article 14 of the Directive, as it is for the right to appeal for damages

suffered, provided for in articles 22 and 23 of this.”

The general objective of the right of access is to provide individuals with information

sufficient, transparent and easily accessible information about the processing of your data

personal so that they can know and verify the legality of the treatment and the accuracy

of the processed data.

Unless expressly indicated otherwise, the request must be understood in the

sense that it refers to all personal data relating to the interested party.

"Thus, if full access is not given, the data subject must be informed of the reasons and specific circumstances that allow knowing the reasons in case the claimant wishes to take measures against that consideration", as indicated in point 172 of the aforementioned Directives 1/2022. The data controller must search for personal data in all computer systems and in non-computer files on the basis of search criteria that reflect the way the information is structured.

In the event that the person in charge is going to apply exceptions or restrictions to the right of access should carefully check which parts of the information the information refers to. exception and provide all information that is not excluded by the exception. This forecast would be part of the data processing from the design, having established previously said aspect sufficiently developed, explicit and documented.

The communication of data and other complementary information about the treatment must be provided in a concise, transparent, intelligible and easily accessible form, using a clear and simple language. The more precise requirements in this regard depend on the circumstances of data processing, as well as the ability of the interested party to understand communication.

In this sense, in addition, the access provided on 02/23/2021 is not adequate, for incomplete, it is not the original format, but a summary, with little information and chronologically disordered in the content of the account of the events that appear registered, limiting itself in an unordered way to the grouping of dates and naming of logs, adding an own explanation that given the diversity and the The nature of the situations that may arise does not even minimally satisfy the content of the right of access.

Differs from the one provided on 12/14/2021 in that the latter is the original format and containing all the features of the log. However, the claimed party has not included all the logs, since what he calls “technical” logs are missing, also resulting in that are incomprehensible in attention to the keys and abbreviations that appear in document whose meaning is unknown.

Thus, and notwithstanding the foregoing, if the data consists of "codes" as in this case, or other “raw data” from the service, must be explained to make sense to the interested. No such explanation has been supplied in the disclosure provided on 12/14/2021.

Access to personal data means access to actual personal data, not only a general description of the data nor a mere reference to the categories of personal data processed by the data controller.

Raw data could be explained as unanalyzed data underlying a treatment. Raw data can exist at different levels, where the highest level is data base can only be machine readable (as "bits"). It should be noted that the Information provided to the interested party must always be in a format readable by the user. human.

Because all the logs appear in a single block referring to the claiming device, both the so-called technical logs and those that were considered personal data by the claimed party, have for their complete understanding various columns with various descriptors that need to be deciphered, the translation of the keys to all logs.

When providing data in a raw format, it is important that the data controller adopt the necessary measures to ensure that the data subject understands the data, for example, by providing an explanatory document that translates the raw format into a format easy to use slider. In addition, it could be explained in such a document what the abbreviations and other acronyms.

Regarding the application of article 15.4 of the GDPR, reference is made to the condition as to the modality of care of the right of access in order to reconcile the rights in conflicts with the claimed party, given that it should not affect the right of access itself as we have indicated previously.

It should be taken into account that the GDPR has established that the right of access includes provide complete information.

The condition provided for in article 15.4 of the GDPR, would be restricted only to the delivery of a copy to the party claiming the data that may be affected by the trade secret, that is to say to part of its content. Thus, the claimant can receive the response of the exercise use of the right of access in another modality that is not the copy, or even combining several modalities if the circumstances require it, as in this case of rights that They can converge in divergences of interests.

It follows that since the content of all the logs is completed with the keys, table descriptions, comments, events, etc., the secret can be revealed all the logs according to the thesis of the defendant. Security-sensitive content to the When dealing with the circumstances that arise with the devices can affect both log types.

There is a key for “(...) of the signal”, a description, and another somewhat broader one in the field. type “***COLUMN.2 (...)”, “***COLUMN.1”, “event” etc common elements with the data personal data, but it is not appreciated what would be such a trade secret, or "know how" in awareness of the performance of events that could jeopardize safety. of the measures of the claimed. In any case, this must be subject to interpretation. restrictive. Thus, the risk to trade secrets, or more specifically, the risk that log the way of acting of the complaining party is revealed, it must be sufficiently

shown case by case that it affects, or can affect. There may be times when a

only indicative of indications of such knowledge or it may be that even with several keys they do not

any secret is revealed.

As a way of respecting the "know how" of the defendant, you can, exceptionally, if

If applicable, justify the reason why additional joint information complementary to

each log that forms the access table, or the joint keys of the same must not

be provided in copy mode. This is in relation to considering that if

certify that a specific way of acting in the face of an event that could

repercussions that the "know how" could be known unjustifiably.

In conclusion,

1. The complaining party has the right to access all the logs, which are their data

personal.

2. Two combined and complementary access modalities are established. and it in

attention to the consideration of the rights and interests concerned, taking into account

Consider also the right of the claimed party to trade secret.

3. A modality of access is the copy.

Taking into account the right of the claimed party to trade secret, in

virtue of art. 15.4 of the GDPR, the content of the copy containing all the

logs.

The limitation to the modality of the right of access to the copy, implies, in this case, not provide the claimant with data on the content of the logs in those cases in which

may be affected by trade secret. The claimed party must justify such

affectation.

4. In the other modality, and complementary, to the previous one, the claimed party will have to

enable a form of access to all the personal data of the claimant, affected or

not for commercial secret, without prejudice to what is established for copying.

5. In both modes of access, personal data must be provided in

original format, understandable and intelligible, with complementary information for its

comprehension.

VIII

From the analysis of the specific case examined and taking into account the circumstances

specific facts revealed throughout the administrative file, of what is

delivered to the claimant, of its content and scope, Securitas has provided under

of what was previously resolved by the AEPD, the "logs" raw, untreated, but having

previously filtering the "logs" and excluding the information that it considers to be not

personal data "since it is exclusively technical information" and abiding by

trade secret.

Likewise, of the logs that it considers contain personal data of the claimant

did not provide the indicatives and keys that would make it possible to fully know their

meaning.

It is considered that the claimed party has breached the resolution of the Spanish Agency

of Data Protection in relation to the measures imposed on it.

The facts are considered to constitute an infringement, attributable to the claimed party,

for violation of article 58.2.c) of the GDPR, which provides the following:

"2. Each control authority will have all the following corrective powers

indicated below:

"c) order the person in charge or person in charge of the treatment to attend to the requests for

exercise of the rights of the interested party under this Regulation

This infringement is typified in article 83.6 of the GDPR, which stipulates the following:

"Failure to comply with the resolutions of the control authority under article 58,

section 2, will be penalized in accordance with section 2 of this article with fines

administrative costs of a maximum of EUR 20,000,000 or, in the case of a company, a

amount equivalent to a maximum of 4% of the total global annual turnover of the

previous financial year, opting for the one with the highest amount.”

That authorizes the AEPD to proceed in accordance with the power granted by article 58.2

“i) impose an administrative fine in accordance with article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each case

particular;"

In this case, it proceeds due to the lack of attention to comply with its terms, scope and

content the essential content of the right of access, and for the impediment that

deprive of the data that is the object of treatment, an administrative fine.

Article 71 of the LOPDGDD indicates:

"Infractions are the acts and conducts referred to in sections 4, 5 and

6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to

the present organic law.”

For the purposes of the limitation period for infringements, the alleged infringement prescribes

three years, in accordance with article 72.1 of the LOPDGDD, states:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are considered very serious and will prescribe after three years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the

following:”

"m) Failure to comply with the resolutions issued by the authority for the protection of

competent data in exercise of the powers conferred by article 58.2 of the

Regulation (EU) 2016/679.”

IX

The fine imposed must be, in each individual case, effective, proportionate and

dissuasive, in accordance with the provisions of article 83.1 of the GDPR. Consequently, it

must graduate the sanction to be imposed in accordance with the criteria established by the

Article 83.2 of the GDPR, and with the provisions of Article 76 of the LOPDGDD, regarding the

section k) of the aforementioned article 83.2 of the GDPR.

The following circumstances are taken into consideration:

-Article 83.2.a) "the nature, seriousness and duration of the infringement, taking into account

the nature, scope or purpose of the processing operation in question

such as the number of interested parties affected and the level of damages that have

suffered;”

On the occasions that access was provided, the first two with the same content,

and a third after the resolution of the procedure for the exercise of rights was

incomplete, not partial, since neither all of its content is reflected nor is its content provided.

comprehension. These are data processing operations, in a matter such as related to home security. Such elements would operate as aggravating factors. Failure to comply with the obligation to attend to the right cannot have the same consequences depending on the duration, persistence of the negative reasons or repeated responses, accrediting in this case a greater seriousness that qualifies the sanctioning response.

-Article 83.2.b) of the GDPR, "intentionality or negligence in the infringement" that is states that on 09/17/2021 the procedure on the exercise of rights was resolved, TD/00167/2021, although appealed in replacement, on 10/27/2021 confirms the resolution of the TD, notified the day after the claim. There is no record that he complied with the attention of the right within the term granted in the resolution, which exceeds widely, and which only after the claimant makes the mandatory declaration of not having received anything at the In this regard, the AEPD had to contact the defendant who, only then, agreed to send you the last letter of 12/14/2021, which continues without satisfying the content of the right. The action denotes a clear negligence in the fulfillment of the duty that corresponds.

The defendant states that she acts diligently when hiring an entity to study the logs in their relationship with personal data in order to meet the request of the claimant

Regarding this statement, it seems to contradict another that the defendant pointed out in allegations to the same initiation agreement, that the contracting of the legal service that was embodied in the report of document 1, it was done mainly for the purpose of compliance normative that foresees assessing what data is being processed. Being the logs common data to all products derived from an alarm, which manages the claimed, from the entry into force of the GDPR should have implemented the treatment from the design that has been mentioned in the resolution, in order for the person in charge to put into technical and organizational measures to implement the principles and safeguards of individual rights. In essence, this means that you must integrate the data protection in its processing activities and commercial practices, from the design stage and throughout the life cycle. Helps make sure you meet fundamental principles and requirements of the GDPR, and is part of the approach of responsibility. This supposed diligence is neither more nor less than the fulfillment that the regulations establish.

-Article 76.2 b) of the LOPDGDD: "The link between the offender's activity and the processing of personal data". The defendant has products What offer for those who are essential their usual management of data processing that they appear listed in contracts next to their devices.

Regarding the allegations with which the defendant intends to mitigate the penalty for state that he attended, although partially the right, on three occasions, it must be indicate that the access of 02/23/2021, reproduced on 05/18/2021 are mere accesses repeated formals, own elaborations with a log description with explanation generic, attention that is incomplete, not partial. Not only is it not from the original, it's a elaboration of the claimed, it lacks the keys for its understanding and the description of the events, but also does not include the logs that the defendant calls improperly "technical". In addition, deducing that it has been a partial compliance, tries to tie the consequence that access is a minor non-compliance to the effects of the prescription of article 74.c) of the LOPDGD. On the contrary, the offense in such a way, both as a result of accesses with the same content, as the one that has

place with the one provided on 12/14/2021, it must be qualified as substantial, ruling out its

even formal character, at least "merely formal", having an impact on the fact that it had no

nor has he had access to all the information and the repercussions it has for the affected party.

Regarding the alleged good faith, "it has been complied with up to three times", it is considered

that it is not important the times in which compliance is given, because with one it would be

sufficient, estimating that the occasions in which it has been provided have been with

incomplete content, not partial as claimed. On the other hand, good faith does not

certifies the absence of guilt and illegality.

It is considered that based on the aforementioned factors, due to the infringement of article

58.2 of the GDPR, it is agreed to impose a fine of 50,000 euros.

X

As corrective power, it corresponds to this AEPD: "order the person in charge or in charge

of the treatment that meet the requests for the exercise of the rights of the interested party in

under this Regulation". (Article 58.2.c) of the GDPR)

The defendant must complete the requested access, providing all the logs it has

excepted to date, including all the logs contained by

chronological order in document 2 of the table provided in the allegations to the agreement

beginning, which were marked in red, in which they complement each other and succeed each other.

logically the device registers.

The information must contain the keys that allow clarifying the aforementioned table and its

sections that make the data tables understandable in line format or in

gross as obtained by the defendant.

The specificities of the foundation of law VI and VII will be taken into account as

mode of compliance with the measure imposed.

The imposition of this measure is compatible with the sanction consisting of a fine administration, according to the provisions of art. 83.2 of the GDPR.

It is noted that not meeting the requirements of this body may be

considered as an administrative offense in accordance with the provisions of the GDPR,

classified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the

opening of a subsequent administrative sanctioning procedure.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE SECURITAS DIRECT ESPAÑA, S.A., with NIF A26106013, for

an infringement of article 58.2 c) of the GDPR, typified in article 83.6 of the aforementioned

GDPR, and qualified, for the purposes of prescription as serious in article 72.m) of the

LOPDGDD, an administrative sanction of 50,000 euros.

SECOND: Pursuant to article 58.2.c) of the GDPR, which authorizes to “order the

person in charge or person in charge of the treatment that attends to the requests for the exercise of the

rights of the interested party under this Regulation;” you are required to in the

within fifteen days attends to the right that is the subject of this claim in the manner indicated.

Failure to comply with the provisions could lead to the exercise of the power

sanctioning in accordance with the provisions of article 83.6 of the GDPR.

THIRD: NOTIFY this resolution to SECURITAS DIRECT ESPAÑA, S.A.

FOURTH: Warn the penalized person that they must make the imposed sanction effective once

that this resolution be enforceable, in accordance with the provisions of art.

98.1.b) of the LPACAP within the voluntary payment period established in art. 68 of the General Collection Regulations, approved by Royal Decree 939/2005, of 07/29, in relation to art. 62 of Law 58/2003, of 12/17, by entering it, indicating the NIF of the sanctioned party and the number of the procedure that appears in the heading of this document, in the restricted account IBAN number: ES00-0000-0000-0000-0000-0000, open in the name of the Spanish Data Protection Agency in the bank CAIXABANK, S.A. Otherwise, it will be collected in the period executive.

Once the notification has been received and once executed, if the execution date is between on the 1st and 15th of each month, both inclusive, the period for making the voluntary payment It will be until the 20th day of the following or immediately following business month, and if it is between on the 16th and last day of each month, both inclusive, the payment period will be until the 5th of second following or immediately following business month.

Against this resolution, which puts an end to the administrative process in accordance with art. 48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the Interested parties may optionally file an appeal for replacement before the Director of the Spanish Agency for Data Protection within a period of one month from the day following the notification of this resolution or directly contentious appeal before the Contentious-Administrative Chamber of the National Court, in accordance with the provisions of article 25 and section 5 of the additional provision fourth of Law 29/1998, of 13707, regulating the Contentious Jurisdiction-administration, within a period of two months from the day following the notification of this act, as provided in article 46.1 of the aforementioned Law.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP, may provisionally suspend the firm resolution in administrative proceedings if the interested party expresses its intention to file a contentious-administrative appeal. If this is the one case, the interested party must formally communicate this fact by writing to the Spanish Data Protection Agency, presenting it through the Registry Email from the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other records provided for in art. 16.4 of the aforementioned LPCAP. Also must transfer to the Agency the documentation that proves the effective filing of the Sponsored links. If the Agency were not aware of the filing of the contentious-administrative appeal within a period of two months from the day following the notification of this resolution, would terminate the suspension precautionary

Mar Spain Marti

Director of the Spanish Data Protection Agency