936-031219

 Procedure No.: PS/00122/2020

RESOLUTION R/00284/2020 TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

In sanctioning procedure PS/00122/2020, instructed by the Agency

Spanish Data Protection Agency to SAUNIER-TEC, HEAT MAINTENANCE

Y FRIO, S.L, in view of the complaint filed by A.A.A., and based on the following,

BACKGROUND

FIRST: On June 16, 2020, the Director of the Spanish Agency for

Data Protection agreed to initiate sanctioning proceedings against SAUNIER-TEC,

MANTENIMIENTOS DE CALOR Y FRIO, S.L (hereinafter, the claimed party), through the

Agreement that is transcribed:

<<

Procedure No.: PS/00122/2020

AGREEMENT TO START A SANCTION PROCEDURE

Of the actions carried out by the Spanish Agency for the Protection of

Data and based on the following

FACTS

FIRST: Ms. A.A.A. (hereinafter, the claimant) on 10/16/2019 filed

claim before the Spanish Data Protection Agency. The claim is

directed against SAUNIER-TEC, MANTENIMIENTOS DE CALOR Y FRIO, S.L with NIF

B81405128 (hereinafter, the claimed one). The grounds on which the claim is based are:

that in mid-October 2019 he received a series of emails with content from

request to change personal data, from accounts with an extension of

domain other than ***DOMAIN.1 which indicates that it is possible that they are not emails

officers sent by the Sauniertec company; that in the aforementioned emails their

personal data and full bank account number; also contain a



attachment that did not proceed to open; who contacted the company

Sauniertec asking if his database had been hacked, to which he

they answer yes; After the affirmation, he asked that the person be contacted.

data protection officer without them having responded to your request; that

considers that this situation is especially serious since it is proof that the

hackers have in addition to your personal data, your bank details and could

proceed to generate fraudulent charges.

SECOND: Upon receipt of the claim, the Subdirectorate General for

Data Inspection proceeded to carry out the following actions:

On 11/22/2019, the claim submitted was transferred to the defendant for analysis

and communication to the affected party of the decision adopted in this regard. Likewise, it

required so that within a month it would send to the Agency determined

information:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

- Report on the causes that have motivated the incidence that has originated the

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents.

- Any other that you consider relevant.

The one claimed by letter of 12/12/2019 answered the questions

raised by the AEPD in its request for information on the incidence of

security produced. It also indicated that a communication had been sent to the

claimant in this same sense, accrediting its receipt and providing:

-

GDPR Risk Report October 2019 Saunier-Tec.

- Procedure for Risk Assessment and Notifications of Violations of

Saunier-Tec Security.



-

Security incident report in a mailbox with the measures

implemented techniques.

- Contract to carry out a Cybersecurity Audit

- Saunier-Tec customer response

THIRD: On 03/31/2020, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed by the claimant against the respondent.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

The Director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.



Article 58 of the RGPD, Powers, states:

II

"two. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

i) impose an administrative fine under article 83, in addition to or in

Instead of the measures mentioned in this section, according to the

circumstances of each particular case;

(…)”

The RGPD establishes in article 5 of the principles that must govern the

treatment of personal data and mentions among them that of "integrity and

confidentiality”.

The article notes that:

"1. The personal data will be:

(…)

f) treated in such a way as to ensure adequate security of the

personal data, including protection against unauthorized or unlawful processing and

against its loss, destruction or accidental damage, through the application of measures

appropriate technical or organizational ("integrity and confidentiality").

In turn, the security of personal data is regulated in articles

32, 33 and 34 of the RGPD.



Article 33 of the RGPD, Notification of a breach of the security of the

personal data to the control authority, establishes that:

"1. In case of violation of the security of personal data, the

responsible for the treatment will notify the competent control authority of

accordance with article 55 without undue delay and, if possible, no later than 72

hours after you become aware of it, unless it is unlikely

that said breach of security constitutes a risk to the rights and

freedoms of natural persons. If the notification to the control authority does not have

place within 72 hours, must be accompanied by an indication of the reasons for

the procrastination

2. The person in charge of the treatment will notify the person in charge without undue delay

of the treatment the violations of the security of the personal data of which

be aware.

3. The notification referred to in section 1 must, at a minimum:

a) describe the nature of the data security breach

including, where possible, the categories and approximate number of

affected stakeholders, and the categories and approximate number of data records

affected personnel;

b) communicate the name and contact details of the data protection delegate

data or another point of contact where further information can be obtained;

c) describe the possible consequences of the breach of the security of the

personal information;

d) describe the measures adopted or proposed by the person responsible for the

treatment to remedy the violation of the security of personal data,

including, if applicable, the measures adopted to mitigate the possible effects

negatives.

4. If it is not possible to provide the information simultaneously, and to the extent

where it is not, the information will be provided gradually without undue delay.



5. The data controller will document any violation of the

security of personal data, including the facts related to it, its

effects and corrective measures taken. Such documentation will allow the

control authority verify compliance with the provisions of this article.

And article 34, Communication of a breach of data security

data to the interested party, establishes that:

"1. When the data security breach is likely

entails a high risk for the rights and freedoms of individuals

physical data, the data controller will communicate it to the interested party without delay

improper.

2. The communication to the interested party contemplated in section 1 of this

article will describe in clear and simple language the nature of the violation of the

security of personal data and will contain at least the information and

measures referred to in article 33, section 3, letters b), c) and d).

3. The communication to the interested party referred to in section 1 will not be

required if any of the following conditions are met:

a) the data controller has adopted technical protection measures

and organizational measures and these measures have been applied to the data

affected by the violation of the security of personal data,

in particular those that make personal data unintelligible for

anyone who is not authorized to access them, such as encryption;

b) the data controller has taken further steps to ensure

that there is no longer the probability that the high risk for the

rights and freedoms of the interested party referred to in section 1;

c) involves a disproportionate effort. In this case, you will choose instead

by a public communication or similar measure by which it is reported

equally effectively to stakeholders.



4. When the person in charge has not yet communicated to the interested party the

violation of the security of personal data, the control authority, once

Considering the probability that such a violation involves a high risk, it may require

to do so or may decide that any of the conditions mentioned in

section 3”.

The violation of articles 33 and 34 of the RGPD is typified in the

article 83.4.a) of the aforementioned RGPD in the following terms:

"4. Violations of the following provisions will be sanctioned, in accordance

with paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or,

in the case of a company, an amount equivalent to a maximum of 2% of the

global total annual turnover of the previous financial year, opting for

the largest amount:

a) the obligations of the person in charge and the person in charge pursuant to articles 8,

11, 25 to 39, 42 and 43.

(…)

For its part, the LOPDGDD in its article 71, Violations, states that:

“The acts and behaviors referred to in the regulations constitute infractions.

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

Article 73, for prescription purposes, qualifies as "Infringements considered

serious:



Based on the provisions of article 83.4 of Regulation (EU) 2016/679

are considered serious and will prescribe after two years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

r) Failure to comply with the duty to notify the data protection authority

data of a breach of security of personal data in accordance with the

provided for in article 33 of Regulation (EU) 2016/679.

(…)

And in its article 74, for the purposes of prescription, it qualifies as "Infringements

considered mild:

They are considered minor and the remaining infractions of a character will prescribe after a year.

merely formal of the articles mentioned in paragraphs 4 and 5 of article 83

of Regulation (EU) 2016/679 and, in particular, the following:

(…)

ñ) Failure to comply with the duty to notify the affected party of a violation of

the security of the data that entails a high risk for the rights and freedoms of

those affected, as required by article 34 of Regulation (EU) 2016/679,

unless the provisions of article 73 s) of this organic law are applicable.

(…)

The facts revealed in this claim are specified in

the existence of a security breach in the systems of the claimed

breaching the duty to communicate both to the data protection authority

personal as to the interested parties the violation of the security of their data.

III



The GDPR defines personal data security breaches as

“all those violations of security that cause the destruction, loss or

accidental or unlawful alteration of personal data transmitted, stored or processed

otherwise, or unauthorized communication or access to such data”.

In the present case, within the framework of file E/10606/2019, the AEPD requested

to the claimed an informative requirement.

The responsibility of the claimed party is determined by the incidence of

security revealed by the claimant, since it is responsible for taking

decisions aimed at effectively implementing technical measures and

appropriate organizational measures to guarantee a level of security appropriate to the risk to

in order to guarantee the confidentiality of the data and, among them, those aimed at restoring

its availability and access to data quickly in the event of a physical incident or

technical..

From the documentation provided, it can be deduced that the entity failed to comply with that

obligation as evidenced by the emails with change request content

of personal data from accounts with a domain extension other than

@sauniertec.com, confirming the attempted hacking of customer accounts,

the entity itself acknowledging the error in the management of the claimant's request as well

such as the existence of malware in the email account of a worker

impersonating her identity and using emails that had been sent to her.

It is true that the respondent who was aware of the incident adopted measures aimed at

remedy it, however the RGPD regulates in its article 33 the notification

security breaches that may pose a risk to the rights and

freedoms of natural persons to the competent supervisory authority, which in the case

Spanish is about the AEPD.

Therefore, whenever a gap or incident of this type is seen as

affected personal data of natural persons we must communicate it to the

AEPD and, in addition, we must notify it within a maximum period of 72 hours from

as long as we are aware of the breach.



There is also no evidence that, in accordance with what is stated in the

article 34 had the affected interested parties been informed of the violation of the

security of your personal data, but after analyzing the facts and according to the

internal procedure of Risk Assessment and Notifications of Violations of

Security determined that it was not necessary to make such communications.

In accordance with the foregoing, it is estimated that the respondent would be

allegedly responsible for the infringement of articles 33 and 34 of the RGPD,

violation that is typified in article 83.4.a) of the RGPD.

IV

In order to establish the administrative fine to be imposed,

observe the provisions contained in articles 83.1 and 83.2 of the RGPD, which

point out:

"1. Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

Regulation indicated in sections 4, 5 and 6 are in each individual case

effective, proportionate and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances

of each individual case, in addition to or as a substitute for the measures contemplated

in article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case will be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the

nature, scope or purpose of the processing operation in question

as well as the number of stakeholders affected and the level of damage and

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;



d) the degree of responsibility of the person in charge or of the person in charge of the

treatment, taking into account the technical or organizational measures that have

applied under articles 25 and 32;

e) any previous infraction committed by the person in charge or the person in charge of the

treatment;

f) the degree of cooperation with the supervisory authority in order to put

remedying the breach and mitigating the possible adverse effects of the breach;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in

particular if the person in charge or the person in charge notified the infringement and, in such case,

what extent;

i) when the measures indicated in article 58, paragraph 2, have been

previously ordered against the person in charge or the person in charge in question

in relation to the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or mechanisms

certificates approved in accordance with article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the

case, such as financial benefits realized or losses avoided, direct

or indirectly, through infringement.

In relation to letter k) of article 83.2 of the RGPD, the LOPDGDD, in its

Article 76, “Sanctions and corrective measures”, establishes that:

"two. In accordance with the provisions of article 83.2.k) of the Regulation (EU)

2016/679 may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of treatments

of personal data.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

commission of the offence.



e) The existence of a merger by absorption process after the commission

of the infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when it is not mandatory, a delegate for the protection of

data.

h) The submission by the person in charge or person in charge, with

voluntary, to alternative conflict resolution mechanisms, in those

assumptions in which there are controversies between those and any

interested."

In accordance with the transcribed precepts, and without prejudice to what may result

of the instruction of the procedure, in order to set the amount of the sanction to

impose in the present case for the infringement typified in article 83.4 of the RGPD of

which the defendant is held responsible, in an initial assessment, are estimated

concurrent the following factors:

The defendant's conduct is the result of a lack of diligence in the

compliance with the obligations imposed by the regulations for the protection of

data.

The nature and severity of the breach, declared security breach.

The absence of notification to the control authority about the facts

produced.

The absence of notification to the interested parties of the possible affectation to their

rights given the category of affected data, bank details.

The number of people affected by the breach.



The degree of responsibility of the data controller, taking into account

the technical or organizational measures applied and that were violated, as well

as the category of affected data.

The activity of the allegedly infringing entity is linked to the

data processing of both customers and third parties.

The volume of business of the claimed.

For all these reasons, an amount of the sanction is established for violation of the

articles 33 and 34 of the RGPD of 6,000 euros.

Therefore, as stated,

By the Director of the Spanish Data Protection Agency,

HE REMEMBERS:

1.

START SANCTION PROCEDURE

to SAUNIER-TEC,

HEAT AND COLD MAINTENANCE, S.L. with NIF B81405128, for the alleged

infringement of articles 33 and 34, sanctioned in accordance with the provisions of article

83.4.a) of the aforementioned RGPD.

2. APPOINT Instructor to B.B.B. and Secretary to C.C.C., indicating that

any of them may be challenged, where appropriate, in accordance with the provisions of the

Articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the Sector

Public (LRJSP).



3. INCORPORATE to the disciplinary file, for evidentiary purposes, the complaint

filed by the complainant and her documentation, the documents obtained and

generated by the Inspection Services during the preliminary investigation phase, as well as

such as the report of previous inspection actions; documents all of them

make up the file.

4. THAT for the purposes provided in art. 64.2 b) of Law 39/2015, of 1

October, of the Common Administrative Procedure of the Public Administrations

(LPACAP), and art. 127 letter b) of the RLOPD, the sanction that for said infractions that

could correspond would be 6,000 euros (six thousand euros), without prejudice to what

result of the instruction.

5. NOTIFY this Agreement to SAUNIER-TEC, MAINTENIMIENTOS DE

HEAT AND COLD, S.L. with NIF B81405128, expressly indicating their right to

hearing in the procedure and granting a hearing period of TEN DAYS

SKILLFUL to formulate the allegations and propose the evidence that it considers

coming. In your brief of allegations you must provide your NIF and the number of

procedure at the top of this document.

Likewise, in accordance with articles 64.2.f) and 85 of the LPACAP,

informs that, if it does not make allegations within the term of this initial agreement, the

The same may be considered a resolution proposal.

You are also informed that, in accordance with the provisions of article

85.1 LPACAP, may acknowledge its responsibility within the term granted for the

formulation of allegations to this initial agreement which will entail a

reduction of 20% of the sanctions that should be imposed in the present

procedure, equivalent in this case to 1,200 euros. With the application of this

reduction, the total sanction would be established at 4,800 euros, resolving the

procedure with the imposition of this sanction.

Similarly, you may, at any time prior to the resolution of the

present procedure, carry out the voluntary payment of the proposed sanctions,

in accordance with the provisions of article 85.2 LPACAP, which will mean a

reduction of 20% of the amount of the same, equivalent in this case to 1,200 euros. With the application of this reduction, the total sanction would be established in 4,800 euros and its payment will imply the termination of the procedure.



The reduction for the voluntary payment of the sanction is cumulative to the one It is appropriate to apply for the acknowledgment of responsibility, provided that this acknowledgment of responsibility is revealed within the period granted to formulate arguments at the opening of the procedure. The pay volunteer of the amount referred to in the preceding paragraph may be made at any time prior to resolution. In this case, if it were appropriate to apply both reductions, the amount of the total sanction would be established at 3,600 euros.

In any case, the effectiveness of any of the two reductions mentioned will be conditioned to the withdrawal or renunciation of any action or resource in via administrative against the sanction.

In the event that you choose to proceed with the voluntary payment of any of the amounts indicated above (4,800 euros or 3,600 euros), in accordance with the provided for in article 85.2 referred to, we indicate that you must make it effective by your deposit in the restricted account number ES00 0000 0000 0000 0000 0000 open to name of the Spanish Data Protection Agency at CAIXABANK Bank, S.A., indicating in the concept the reference number of the procedure that appears in the heading of this document and the reason for the reduction of the amount to which welcomes

Likewise, you must send proof of payment to the General Subdirectorate of

Inspection to proceed with the procedure in accordance with the quantity

entered.

The procedure will have a maximum duration of nine months from the

the date of the start-up agreement or, where applicable, of the draft start-up agreement.

Once this period has elapsed, it will expire and, consequently, the file of

performances; in accordance with the provisions of article 64 of the LOPDGDD.

Finally, it is pointed out that in accordance with the provisions of article 112.1 of the

LPACAP, there is no administrative appeal against this act.



Director of the Spanish Data Protection Agency

>>

: On June 24, 2020, the claimant has proceeded to pay the

SECOND

sanction in the amount of 3600 euros making use of the two reductions provided

in the Startup Agreement transcribed above, which implies the recognition of the

responsibility.

THIRD: The payment made, within the period granted to formulate allegations to

the opening of the procedure, entails the waiver of any action or resource in via

administrative action against the sanction and acknowledgment of responsibility in relation to

the facts referred to in the Initiation Agreement.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of control, and as established in art. 47 of the Organic Law 3/2018, of 5 December, of Protection of Personal Data and guarantee of digital rights (in hereinafter LOPDGDD), the Director of the Spanish Agency for Data Protection is competent to sanction the infractions that are committed against said Regulation; infractions of article 48 of Law 9/2014, of May 9, General Telecommunications (hereinafter LGT), in accordance with the provisions of the article 84.3 of the LGT, and the infractions typified in articles 38.3 c), d) and i) and 38.4 d), g) and h) of Law 34/2002, of July 11, on services of the society of the information and electronic commerce (hereinafter LSSI), as provided in article 43.1 of said Law.

II

Article 85 of Law 39/2015, of October 1, on Administrative Procedure Common to Public Administrations (hereinafter, LPACAP), under the rubric "Termination in sanctioning procedures" provides the following:

"1. A sanctioning procedure has been initiated, if the offender acknowledges his responsibility, the procedure may be resolved with the imposition of the sanction to proceed.

2. When the sanction is solely pecuniary in nature or fits impose a pecuniary sanction and another of a non-pecuniary nature but it has been justified the inadmissibility of the second, the voluntary payment by the alleged perpetrator, in any time prior to the resolution, will imply the termination of the procedure, except in relation to the replacement of the altered situation or the determination of the compensation for damages caused by the commission of the infringement.

3. In both cases, when the sanction is solely pecuniary in nature,

the competent body to resolve the procedure will apply reductions of, at

least 20% of the amount of the proposed sanction, these being cumulative

each. The aforementioned reductions must be determined in the notification of

initiation of the procedure and its effectiveness will be conditioned to the withdrawal or

Waiver of any administrative action or recourse against the sanction.



The reduction percentage provided for in this section may be increased

regulations.

According to what was stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: TO DECLARE the termination of procedure PS/00122/2020, of

in accordance with the provisions of article 85 of the LPACAP.

SECOND:

HEAT AND COLD MAINTENANCE, S.L.

NOTIFY

the present

resolution to

SAUNIER-TEC,

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure Common of the Public Administrations, the interested parties may file an appeal contentious-administrative before the Contentious-administrative Chamber of the National Court, in accordance with the provisions of article 25 and section 5 of the fourth additional provision of Law 29/1998, of July 13, regulating the Contentious-Administrative Jurisdiction, 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.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es