 Procedure No.: PS/00225/2019

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: On 02/05/2019, Mr. A.A.A., on behalf of FACUA - ASSOCIATION OF

CONSUMERS AND USERS IN ACTION (hereinafter FACUA), filed

claim before the Spanish Data Protection Agency. The claim is

directed against HOLALUZ-CLIDOM, S.A., with NIF A65445033 (hereinafter HOLALUZ).

The reasons on which the claim is based are, in summary, the following: the

vulnerability of the website https://www.holaluz.com owned by the company by being

exposed the data associated with the CUPS (Universal Supply Point Code),

hundreds of users; Anyone who accesses the aforementioned website can know

the volume of electrical consumption produced in any building with only

enter the address of the property that interests you and have access to data that

only the owner of the supply should know.

Attached as a single document is a video certified by the company save the

proof.com (which according to its website certifies the content of web pages and files with

legal validity), in which you can see the operation of the web in what is

refers to the above.

Likewise, the claimant provides a document in which he declares that he has sent an e-mail on

01/28/2019 to the respondent in which he reported the facts stated

previously, without a response to it; attach a copy of the email

email, as well as the HOLALUZ social network twitter profile.

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

Data Inspection proceeded to carry out the following actions:

On 02/26/2019, the claim presented was transferred to HOLALUZ for analysis and

communication to the complainant 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 sent to the claimant

regarding the transfer of the claim and proof that the claimant

had received notice of that decision.

- Report on the causes that led to the incident that originated the

claim.

- Inform about the measures adopted to prevent their recurrence.

similar incidents.

- Any other that you consider relevant.

On the same date, the claimant was informed of the receipt of the claim and

its transfer to the claimed entity.

HOLALUZ has not responded to the request for information made by the Agency

Spanish Data Protection.

THIRD: On 05/21/2019, 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 HOLALUZ.

FOURTH: On 10/04/2019, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged infringement for the alleged infringement of article 32.1, 33 and 34 of the RGPD sanctioned in accordance with the provisions of article 83.4.a) of the aforementioned Regulation.

FIFTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written allegations on 07/10/2019 stating, in summary, the following: that on the date 12/16/2019 the company CLIDON carried out the transformation from SL to SA and the modification of its corporate name, becoming HOLALUZ CLIDON;

the error attributed to the alleged lack of notification of the security breach of personal data, not being true since it was presented on 02/15/2019; the compliance with data protection regulations by the entity having established adequate security measures; the absence of infringement of article 32.1 of RGPD; compliance with the duty to notify the existence of the security breach; the absence of obligation in the duty to notify the breach of security to the interested parties; compliance with the duty of collaboration and management of the security breach; the request for file of the procedure.

SIXTH: On 12/19/2019, the opening of a practice period for tests, remembering the following:

- Consider reproduced for evidentiary purposes the claim filed by FACUA - ASSOCIATION OF CONSUMERS AND USERS IN ACTION and its documentation, the documents obtained and generated by the Services of Inspection that are part of file E/02128/2019.
- Consider reproduced for evidentiary purposes, the allegations to the initial agreement PS/00225/2019 presented by CLIDOM ENERGY S.L. (HELLOLIGHT), and the accompanying documentation.
- By diligence of the instructor, impressions of the HOLALUZ website screen.

SEVENTH: On 06/29/2020, a Resolution Proposal was issued in the sense of

that the Director of the AEPD file the claimant for the alleged violation

of articles 32.1, 33 and 34 of the RGPD, typified in article 83.4.a) of the aforementioned

Regulation.

After the period established for this purpose, the respondent has not submitted a written

allegations at the time of issuing this resolution.

EIGHTH: Of the actions carried out, the following have been accredited

proven facts:

PROVEN FACTS

FIRST. FACUA, by means of a letter dated 02/05/2019, filed a claim with the

Spanish Data Protection Agency against HOLALUZ, as a consequence of the

vulnerability of the website https://www.holaluz.com when the data is exposed

associated with the CUPS of hundreds of users and that anyone who

access the aforementioned website may have knowledge of the electricity consumption that is

occurs at any of the addresses by simply entering the address of the

same.

SECOND. It consists provided by FACUA video certified by the company SAVE THE

PROOF in which you can see the operation of the web in which

specifies step by step what is described in the previous point.

THIRD. It is accredited that FACUA sent HOLALUZ on 01/28/2019 email

email informing of the facts discovered, stating that there has been no

response to it and not knowing if technical action has been carried out to

rectify the alleged facts.

FOURTH. There is evidence of the deed of transformation of the limited company in

corporation, as well as the modification of its corporate name through

public deed, of CLIDOM ENERGY S.L. of 09/16/2019, being renamed

HOLALUZ CLIDOM, S.A.

FIFTH. It is accredited that HOLALUZ on 02/15/2019 notified the AEPD

breach of confidentiality that occurred on 02/14/2019, attaching proof of

presentation of the security breach notification and the annex to the notification of

the same in which it is accredited to have adopted measures of a technical nature and

organizational. It is also recorded that HOLALUZ sent FACUA an email of

02/18/2019 informing of the measures adopted to resolve the incident of

claimed security.

FOUNDATIONS OF LAW

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.

Yo

II

Article 32 of the RGPD "Security of treatment", establishes that:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

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

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration shall be given to

taking into account the risks presented by the processing of data, in particular as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The person in charge and the person in charge of the treatment will take measures to

guarantee that any person acting under the authority of the controller or the

manager and has access to personal data can only process said data

following the instructions of the person in charge, unless it is obliged to do so by virtue of the

Law of the Union or of the Member States".

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 number

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

of affected personal data records;

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

processing to remedy the data security breach

including, if applicable, the measures taken to mitigate the

possible negative effects.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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 delay

improper.

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 GDPR defines security breaches of personal data as

those incidents that cause the accidental destruction, loss or alteration or

illicit personal data, as well as unauthorized communication or access to the

themselves.

III

Since last 05/25/2018, the obligation to notify the Agency of breaches

or security breaches that could affect personal data is applicable to

any controller of personal data processing, which underlines the

importance that all entities know how to manage them.

Consequently, as soon as the data controller has
knowledge that a data security breach has occurred
must, without undue delay and, if possible, no later than 72 hours
after you have become aware of it, notify the security breach of
personal data to the competent control authority, unless the
responsible can demonstrate, in accordance with the principle of proactive responsibility, the
Unlikely that the breach of the security of the personal data will entail a
risk to the rights and freedoms of natural persons.
The data controller must inform the interested party without delay
improper violation of the security of personal data in the event that it may
pose a high risk to your rights and freedoms, and allow you to take the
necessary precautions. The communication must describe the nature of the violation
of the security of personal data and the recommendations so that the person
affected physical condition mitigates the potential adverse effects resulting from the violation.
Said communications to the interested parties must be made as soon as possible.
reasonably possible and in close cooperation with the supervisory authority,
following its guidelines or those of other competent authorities, such as the
police authorities. Thus, for example, the need to mitigate a risk of damage and
immediate damages would justify a quick communication with the interested parties,
while it is possible to justify that the communication takes more time due to the need to
apply appropriate measures to prevent data security breaches
continuous personal or similar.

It should also be noted, that notification of a security breach

implies analyzing the diligence of the person in charge or, where appropriate, in charge/s and the measures

applied.

Article 33 of the RGPD establishes the way in which a notification must be made.

violation of the security of personal data to the control authority.

And article 34 of the mentioned Regulation indicates when it is necessary

report a violation of the security of personal data to the interested party.

In this same sense, it is stated in Recitals 85 and 86 of the RGPD:

(85) If adequate measures are not taken in time, violations of the

security of personal data can lead to physical damage,

material or immaterial for natural persons, such as loss of control over their

personal data or restriction of their rights, discrimination, usurpation of

identity, financial loss, unauthorized reversal of pseudonymization, damage

for reputation, loss of confidentiality of data subject to professional secrecy,

or any other significant economic or social damage to the natural person in

question. Consequently, as soon as the data controller has

knowledge that a data security breach has occurred

personal data, the controller must, without undue delay and, if possible, no later than

72 hours after you have been aware of it, notify the violation of the

security of personal data to the competent control authority, unless

the person in charge can demonstrate, in accordance with the principle of proactive responsibility,

the improbability that the breach of the security of the personal data will entail

a risk to the rights and freedoms of natural persons. yes said

notification is not possible within 72 hours, it must be accompanied by a

indication of the reasons for the delay, information being able to be provided in phases without

more undue delay.

(86) The controller must notify the data subject without delay

improper violation of the security of personal data in the event that it may

pose a high risk to your rights and freedoms, and allow you to take the

necessary precautions. The communication must describe the nature of the violation

of the security of personal data and the recommendations so that the person

affected physical condition mitigates the potential adverse effects resulting from the violation.

Said communications to the interested parties must be made as soon as possible.

reasonably possible and in close cooperation with the supervisory authority,

following its guidelines or those of other competent authorities, such as the

police authorities. Thus, for example, the need to mitigate a risk of damage and

immediate damages would justify a quick communication with the interested parties,

while it is possible to justify that the communication takes more time due to the need to

apply appropriate measures to prevent data security breaches

continuing personal or similar.

IV

In the present case, the claimed facts suggested that on the website

ownership of the claimant had been exposed the data associated with the CUPS of

hundreds of users; the claimant states that any person who accessed

to the aforementioned website could know the volume of electricity consumption that occurs in

any property by simply entering the address of the property that interests you and

have access to data that only the owner of the supply should know.

Likewise, it was pointed out in Fact Two of the agreement to start the

sanctioning procedure that the respondent had not notified the supervisor of the

bankruptcy that had been revealed to him by the claimant, nor had he given

response to the information request made by the AEPD.

It should be noted that in light of the documents provided, such as the

entity claimed has indicated and this is stated in the proven facts that on 02/15/2019

notified the AEPD of the incident detected and reported by FACUA, attaching the

proof of presentation of the security breach notification and the annex to the

notification accrediting having adopted measures of a technical nature and

relevant organizations.

It also provided the response that was offered to FACUA by email

email dated 02/18/2019 informing them of the situation, despite the fact that FACUA has

pointed out that the merchant had not proceeded to attend to his messages.

In the first place, it should be noted that the transfer of data by the

energy distributors and their subsequent treatment by the

marketers of the energy sector is authorized by Law 54/1997, of

December 27, of the Electricity Sector and in Law 34/1998, of October 7, of the Sector

of hydrocarbons. In accordance with the aforementioned rule, the personal data of the

users could be obtained from supply point databases. The

entities of the sector had to have a database called System of

Supply Point Information (SIPS) containing a series of technical data and

of the holders of the gas and electricity supply points.

Royal Decree 1074/2015, of November 27, which modifies

certain provisions in the electricity sector, established a new wording of the

Article 7 of Royal Decree 1435/2002, of December 27.

In this way, neither the trading companies nor the CNMC can access

from the modification to any information that identifies the holder of the point of

supply, and in particular to the data collected c), z) and aa) of section 1, that is:

“c) Location of the supply point, including full address (type of

street, street name, number, floor and door). This information must refer to all

moment to the point of supply and not to the location, population and province of the holder of

said supply point that is required in letter aa) of this same article.

z) Name and surnames, or where applicable company name and corporate form, of the

owner of the supply point.

aa) Full address of the owner of the supply point. This information

must refer at all times to the owner of the supply point and not to the location,

population and province of said supply point that is required in letter c) of this

same item”

This information continues to be held by the distribution companies, which no longer

will be made available to marketers or the CNMC from that moment.

Therefore, with the new regulation it was not possible to access any information

that directly identifies the owner of the supply point.

The defendant is a company that sells electricity and gas. In

under Royal Decree 1435/2002, of December 27, which regulates the

basic conditions of contracts for the purchase of energy and access to

low voltage networks, and in accordance with the above, has access to the

Supply Point Information System (SIPS), that is, data set

that collects the power, the consumption of the users, etc., so that the

marketers can make personalized offers.

In the present case, so that a client could consult the rate to be contracted

must include in the form that appears on the web page the postal address of the point

of supply or the Unified Code of Supply Point and, selecting the dwelling

or premises in which the client wants to request the supply, the web page processes a

series of data suggesting to the client an estimated fee.

Therefore, the only data that the client accesses when performing the calculation is:

the estimated quota (which is calculated taking into account certain data internally

without the client being able to know them and using a series of algorithms) and CUPS

which is encrypted; in any case once the above measures have been adopted

the volume of consumption of the home or premises, the CUPS number, the

current contracted power, etc.

The respondent has stated that he decided not to include the data of the "power

contracted" in order to protect consumer information, although

has received complaints from its clients for not providing said data since

consider that they need such information for the evaluation of the process of

contracting and the simulation of the estimated quota.

Therefore, through the information provided when performing said calculation,

consumption habits, contracted power, etc. can be known.

On the other hand, the respondent has indicated that access to CUPS, power

contracted, etc. It was only possible with certain knowledge of programming and using malicious mechanisms to obtain information.

However, the respondent had established certain precautions; so in the website interested parties accept, by accessing and using it, the conditions established in the "Legal Notice" indicating in its point 5, that the users of the web undertake to use the website correctly, diligently and lawfully, in accordance with accordance with the law.

There is also no evidence that the information of the users having massively extracted data. The defendant himself has pointed out the impossibility that this could happen by having implemented measures of security that limited in time the number of times that the same IP could consult various offers through the web and by entering different addresses or CUPS and that said verification was carried out by analyzing the evolution of the visits to the website and the hiring form and that there was comparatively no increased but remained constant over time.

Likewise, it is necessary to bear in mind the Judgment of the Contentious-Administrative Court of the National High Court of 02/25/2010 (Appeal 226/2009), in its Foundation of Law Fifth, provides:

“In the present case, the result is the consequence of an activity of intrusion, not protected by legal system and in that sense illegal, of a third party with high computer technical knowledge that breaking the systems of established security accesses the database of registered users in www.portalatino.com, downloading a copy of it. And such facts can be imputed to the appellant entity because, otherwise, the guilt principle.

The principle of guilt, provided for in article 130.1 of Law 30/1992,

provides that they can only be sanctioned for acts constituting an infraction
administrative those responsible for them, even by way of simple non-compliance.
This simple non-observance cannot be understood as the admission in the right
administrative sanction of strict liability, which is proscribed, after
of the STC 76/1999, which stated that the principles of the field of criminal law are
applicable, with certain nuances, in the sanctioning administrative field, requiring
the existence of intent or fault. In this line the STC 246/1991, of December 19,

pointed out that culpability constitutes a basic principle of administrative law
sanctioning Guilt, which does not concur in the conduct analyzed by Portal Latino."
Finally, the respondent created a formal commission to formalize and manage
an action plan adopting a series of measures in order to deal with the
possibility of accessing the information and whose result was the encryption of the
data with the aim that not even a person who acted maliciously and with
willingness to hack the web could have access to CUPS, contracted power and
actual consumption of a dwelling.
Regarding the second of the infractions that the defendant would have committed,
not having proceeded to comply with the obligation to notify the security breach
as required by article 33 of the RGPD, as previously mentioned
It is proven that the notification was carried out through the
Authorized Electronic Address of the AEPD. At the same time, after notification of the
gap and its analysis, a written response was given to the complainant, FACUA.

The third presumed infraction that the defendant would have committed would be the
compliance with the obligation to notify the security breach to the
interested parties, in accordance with article 34 of the RGPD. However, in the
notification of 02/15/2019, the respondent states that he has carried out an internal analysis
determining that the necessary elements did not concur to have to carry out
carry out a notification of the incident to the interested parties, verify that there were no
evidence that information extraction had been carried out and that there was no
a high risk for the rights and interests of those affected.
Therefore, in accordance with the applicable legislation and having assessed the criteria for
graduation of sanctions whose existence has been proven,
The Director of the Spanish Data Protection Agency RESOLVES:
FIRST: FILE HOLALUZ-CLIDOM S.A., with NIF A65445033, for the
alleged infringement of articles 32.1, 33 and 34 of the RGPD, typified in article
83.4 of the GDPR.
SECOND: NOTIFY this resolution to HOLALUZ-CLIDOM S.A., with NIF
A65445033.
In accordance with the provisions of article 50 of the LOPDGDD, the
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 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 reconsideration
before the Director of the Spanish Agency for Data Protection within a period of
month from the day following the notification of this resolution or directly
contentious-administrative appeal 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.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the

LPACAP, the firm resolution may be provisionally suspended in administrative proceedings

if the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

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 Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, it would end the

precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es