 Procedure No.: PS/00118/2020

938-300320

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: The inspection actions are initiated by the reception in this Agency

Spanish Data Protection Agency (hereinafter AEPD) of a written notification

of security breach of personal data sent by the entity IKATZ, S.A. in

quality of data controller, in which it reports that, on July 10

2019, they received an email from the entity in charge of the treatment, to their

once sent to it by INCIBE, reporting a possible intrusion into the systems

information of the investigated.

SECOND: In view of the aforementioned data security breach notification

data, the Subdirectorate General for Data Inspection proceeded to carry out

of previous investigation actions, having knowledge of the following

ends:

BACKGROUND

Security breach notification date: August 28, 2019

INVESTIGATED ENTITIES

During these proceedings, investigations have been carried out on the following

entities:

IKATZ, S.A. (hereinafter IKATZ or investigated entity), with NIF A01043652 and with

address at C/ Arkatxa 1, Pabellón 4 (Pol. Industrial Uritiasolo), 01006 Vitorial-

Gasteiz, Araba-Alava). (tours under the commercial name of Fotoprix)

RESULT OF THE INVESTIGATION ACTIONS

1. Dated September 26 and December 13, 2019, two separate

information requirements to the investigated entity and the responses

received, on October 14, 2019 and January 14, 2020, it follows

the next:

Regarding the data controller. Contracts with companies in charge of

treatment.

The investigated entity, as data controller, has

as corporate purpose the commercialization of photography and telephony material.

It tours commercially under the FOTOPRIX trademark.

It has contracted the entity SPCNET, as the entity in charge of

treatment, hosting of information on its servers.

Regarding the chronology of events. Measures to minimize the incidence.

 On July 9, 2019, at 11:28 p.m., the company SPCNET -where

the information of the investigated entity is hosted - receive an email

email sent by INCIBE informing of a possible intrusion in

the servers that host the information.

 On July 10, 2019, at 9:25 a.m., SPCNET forwards to the entity

investigated the aforementioned email received from INCIBE. The investigated company

confirms the intrusion at 10:30 am when verifying that they had been modified

outdated files installed on one of the machines.

At that time, the files are downloaded for study.

and are deleted in order to eliminate the gateway to the system of

information.

 On July 11, 2019, the investigated party verified that there had been

new modifications so they proceed to restore the systems to date

prior to the estimated date of the intrusion. However, it is found that

the files continue to be modified, so they proceed to restore the

systems with a copy of the latest available backup from mid-June

which contained the files as of March/April, so July 12

block access to the machine from all unauthorized IPs (only

allow access to IPs contained in the Whitelist lists -white lists-).

The investigated entity has provided a copy of the mail sent by INCIBE in which

informs that from the INCIBE CERT there has been knowledge of a possible

security incident pointing to two IP addresses and indicating two addresses

website that have been modified.

Regarding the causes that made possible the incidence

The investigated entity states that surely there have been two

security incidents, the last of which was detected by INCIBE

and was removed with the first system restore in July 2019.

Regarding the previous gap, they state that it is different and they do not know the

access method.

 Regarding the last incident, detected by INCIBE in July 2019, the

investigated entity states that it was due to a vulnerability of the

WORDPRESS (tool for content creation and management

incorporating the typical functionalities of blogs and page creation

commercial websites) that allowed the installation of a plugin (program

computer) which allowed access to the file system and the

code modification.

The investigated entity states that the machine affected by the

security incidents was technically outdated.

Regarding the category of data affected. Notification and indexing

The affected personal data correspond to: name and surnames,

address, mail, DNI, telephone, mobile, date of birth, number of children and

gender.

 The number of customers affected was a maximum of 75,000, of which

15,000 had the DNI.

The investigated entity states that they have no record of the use

by third parties of the possible data obtained through the breach of

security.

The investigated entity states that they have considered that it was not

necessary communication to those potentially affected after assessing the

volume parameters (between 1,000 and 100,000), the type of data

(non-sensitive data) and impact (external) considering a risk (level 18)

indicating that it is not necessary to send communication to clients

affected.

Regarding the security measures implemented prior to the incident

□

The investigated entity has provided a copy of the logs of its information systems.

information.

Regarding the stockings implanted after the incidence

□

The investigated entity states that the

systems, a periodic review is carried out and they have provided a list of the

updates made.

THIRD: On June 9, 2020, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against IKATZ, for the alleged

infringement of articles 32, 33 and 34 of the RGPD, typified in article 83.4 of the

RGPD and as a serious infringement in article 73.f), g), r) and s) of the LOPDGDD.

FOURTH: On 06/16/2020, the start agreement was notified to IKATZ, which did not

filed claims.

PROVEN FACTS

FIRST: On July 10, 2019, IKATZ received an email from the

entity in charge of the treatment (SPCNET), in turn sent to it by INCIBE,

informing of a possible intrusion in the information systems of the investigated.

SECOND: On 07/10/2019, IKATZ confirms that its information system of

customers has been subject to improper access at 10:30 a.m. when verifying that they had

modified outdated files installed on one of the machines

THIRD: Until August 28, 2019, IKATZ did not notify the AEPD of the breach of

security.

FOUNDATIONS OF LAW

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

control, 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

resolve this procedure.

Yo

Article 4.12 of the RGPD establishes that it is considered “violation of the security of the

personal data: any breach of security that results in the destruction, loss

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

otherwise processed, or unauthorized communication or access to said data.”

II

Article 33 of the RGPD establishes the following:

“In case of violation of the security of personal data, the person in charge of the

treatment will notify the competent control authority in accordance with the

article 55 without undue delay and, if possible, no later than 72 hours after

who was aware of it, unless it is unlikely that such violation

constitutes a risk to the rights and freedoms of individuals

physical. If the notification to the supervisory authority does not take place within the period of 72

hours, must be accompanied by an indication of the reasons for the delay."

From the actions carried out, it can be deduced that the investigated entity informed

this Agency on August 28, 2019, almost two months after becoming aware

of the breach of personal data in its information system.

Article 32 of the RGPD, security of treatment, establishes the following:

III

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

of the 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 (The underlining is from the AEPD).

Recital 75 of the RGPD lists a series of factors or assumptions associated with risks to the rights and freedoms of data subjects:

"The risks to the rights and freedoms of natural persons, serious and variable probability, may be due to the processing of data that could cause physical, material or non-material damages, particularly in cases where that the treatment may give rise to problems of discrimination, usurpation of identity or fraud, financial loss, reputational damage, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of the pseudonymization or any other significant economic or social damage; in the cases in which the interested parties are deprived of their rights and freedoms or are prevent exercising control over your personal data; In cases where the data treated personalities reveal ethnic or racial origin, political opinions, religion or philosophical beliefs, militancy in trade unions and the processing of genetic data, data relating to health or data on sex life, or convictions and offenses criminal or related security measures; In cases where they are evaluated personal aspects, in particular the analysis or prediction of aspects related to the performance at work, economic situation, health, preferences or interests personal, reliability or behavior, situation or movements, in order to create or use personal profiles; in the cases in which personal data of vulnerable people, in particular children; or in cases where the treatment involves a large amount of personal data and affects a large number of interested."

In the present case, the investigated entity has not provided the risk analysis of the

treatments for which it is responsible, which prevents the evaluation of the technical and

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

lacking the ability to guarantee the confidentiality, integrity, availability

and resilience of treatment systems and services, which has

caused access by an unauthorized third party to the data stored in your data system.

information.

Article 28 of the LOPDGDD establishes the following:

IV

1. Those responsible and in charge, taking into account the elements

listed in articles 24 and 25 of Regulation (EU) 2016/679, will determine the

appropriate technical and organizational measures that must be applied in order to guarantee and

prove that the treatment is in accordance with the aforementioned regulation, with this law

organization, its implementing regulations and the applicable sectoral legislation. In particular

They will assess whether it is appropriate to carry out the impact assessment on the protection of

data and the prior consultation referred to in Section 3 of Chapter IV of the aforementioned

regulation.

2. For the adoption of the measures referred to in the previous section, the

controllers and processors shall take into account, in particular, the

greater risks that could occur in the following cases:

a) When the treatment could generate situations of discrimination,

identity theft or fraud, financial loss, reputational damage,

loss of confidentiality of data subject to professional secrecy, reversal not

authorized pseudonymization or any other economic, moral or social damage

significant for those affected.

b) When the treatment could deprive those affected of their rights and

freedoms or could prevent them from exercising control over their personal data.

c) When the treatment is not merely incidental or accessory

of the special categories of data referred to in articles 9 and 10 of the

Regulation (EU) 2016/679 and 9 and 10 of this organic law or related data

with the commission of administrative offenses. (...) (The underlining is from the Agency

Spanish Data Protection.).

In the present case, it is clear that the entity in charge of the treatment (SPCNET)

informed in due time and form to the responsible entity (the investigated one) of the same about the

incidence detected in July 2019 by INCIBE.

From the actions carried out, it has been verified that the security measures that

the investigated entity had in relation to the data that it submitted to treatment, not

were appropriate at the time of the security breach.

v

The consequence of this lack of adequate safety measures was exposure to

third parties outside of the personal data of customers. That is, those affected have

seen deprived of control over their personal data.

It should be added that, regarding the possibility of combining information referring to

a holder of personal data, Opinion 4/2007 of the Group can be brought up

of Work of Article 29, “On the concept of personal data” that analyzes the

possibilities of identifying someone through combinations with other

information, starting solely from the data of a client and combining it with

other.

Specifically, it indicates the following: (...) when we speak of "indirectly"

identified or identifiable, we are referring in general to the phenomenon of

"unique combinations", be they small or large. In cases where,

At first glance, the available identifiers do not allow a person to be singled out

determined, it can still be "identifiable", because that combined information

with other data (whether the data controller is aware of them

as if not) will allow to distinguish that person from others. This is where the directive

refers to "one or more specific elements, characteristic of their physical identity,

physiological, psychic, economic, cultural or social. Some of those features

are so unique that they allow effortless identification of a person (the "current

President of the Government of Spain"), but a combination of details

belonging to different categories (age, regional origin, etc.) can also be

quite conclusive in some circumstances, especially if you have access to

additional information of a certain type. This phenomenon has been studied

widely by statisticians, always ready to avoid any

breach of confidentiality (…). So the different pieces come together.

that make up the personality of the individual in order to attribute certain

decisions. (…)

As indicated above, in this case the Internet search, for

example, the name, surnames or email address of any of the

affected can offer results that combining them with those now accessed by

outside third parties, allow us access to other applications of those affected or the

creation of personality profiles, which do not have to have been consented by

its holder.

This possibility supposes an added risk that has to be assessed and that increases the

requirement of the degree of protection in relation to the safety and safeguarding of

integrity and confidentiality of these data.

This risk must be taken into account by the data controller, who in

function thereof, must establish the necessary technical and organizational measures

that prevented the loss of control of the data by the person responsible for the

treatment and, therefore, by the owners of the data that they receive.

they provided.

It establishes article 34 of the RGPD, communication of a violation of the security of

personal data to the interested party, the following:

SAW

"1. When it is likely that the personal data breach

entails a high risk for the rights and freedoms of natural persons, the

responsible for the treatment will communicate it to the interested party without undue delay.

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

describe in clear and plain language the nature of the security breach

of the personal data and will contain at least the information and the measures to

refers to article 33, paragraph 3, letters b), c) and d).

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

one of the following conditions is met:

a) the data controller has adopted technical protection measures and

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

affected by the violation of the security of personal data, in particular

those that make personal data unintelligible to any person who does not

is authorized to access them, such as encryption;

b) the data controller has taken further steps to ensure that

there is no probability that the high risk to 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

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

equally effective to stakeholders.

4. When the person in charge has not yet notified the interested party of the violation of the

security of personal data, the supervisory authority, once considered the

probability that such a violation involves a high risk, it may require you to do so or

may decide that any of the conditions mentioned in section

3".

In the present case, the investigated entity has not provided the risk analysis

associated with the data processing for which it is responsible, although it indicates that it does not

responds to a high level (indicates level 18) so communication to

the interested. However, the investigated entity must be responsible for the

absence of such communication and, where appropriate, of the mandatory impact assessment

according to article 35 of the RGPD, after the new risk assessment required in the

operative part of this Resolution.

Article 71 of the LOPDGDD establishes, under the heading "Infractions" the following:

The acts and behaviors referred to in sections 4, 5 constitute infractions.

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

contrary to this organic law.

7th

It establishes article 73 of the LOPDGDD, under the heading "Infringements considered

serious" the following: Based on the provisions of article 83.4 of the Regulation

(EU) 2016/679 are considered serious and will prescribe after two years the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

f) The lack of adoption of those technical and organizational measures that result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679.

g) The breach, as a consequence of the lack of due diligence, of the

technical and organizational measures that have been implemented as required

by article 32.1 of Regulation (EU) 2016/679.

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

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

Article 33 of Regulation (EU) 2016/679.

In the present case, the infringing circumstances provided for in article 73 concur.

sections f), g) and r) of the LOPDGDD transcribed above.

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III on the "Principles of the power to impose penalties", in article 28

under the heading “Responsibility”, the following:

viii

"1. They may only be sanctioned for acts constituting an infraction.

natural and legal persons administratively, as well as, when a Law

recognize capacity to act, affected groups, unions and entities without

legal personality and independent or autonomous estates, which result

responsible for the same by way of fraud or negligence”

The lack of diligence when implementing security measures from the origin

are the element of culpability that requires the imposition of

sanction.

Article 58.2 of the RGPD, states the following:

IX

2. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

b) sanction any person responsible or in charge of the treatment with

warning when the processing operations have violated the provisions of

this Regulation;

Article 83 of the RGPD, states the following:

(…)

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

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 in accordance with articles 8, 11, 25

at 39, 42 and 43”

Article 76 of the LOPDGDD under the heading "Sanctions and corrective measures",

points out the following:

1. The penalties provided for in sections 4, 5 and 6 of article 83 of the

Regulation (EU) 2016/679 will be applied taking into account the criteria of

graduation established in section 2 of the aforementioned article.

(…)

3. It will be possible, complementary or alternatively, the adoption, when

appropriate, of the remaining corrective measures referred to in article 83.2 of the

Regulation (EU) 2016/679.

X

In the present case, in view of the complexity of the information systems

affected, as well as the actions taken to minimize the consequences

refusals of the aforementioned breach of security of the personal data of its clients,

considers in accordance with the law not to impose a sanction consisting of an administrative fine

and replace it with the penalty of warning in accordance with article 76.3 of the

LOPDGDD in relation to article 58.2 b) of the RGPD.

Therefore, in accordance with the applicable legislation, the Director of the Agency

Spanish Data Protection RESOLVES:

FIRST: IMPOSE IKATZ, S.A., with NIF A01043652, for infraction of the

articles 32 and 33 of the RGPD, typified in Article 83.4 of the RGPD and article 73.f), g) and r) of the LOPDGDD, a sanction of warning.

SECOND: Require IKATZ, S.A. so that within three months he contributes to this AEPD the following documentation:

 Provide a regulated procedure for action and notification to the AEPD before a security incident that allows knowing in a timely manner if it has affected to personal data and that identifies the affected locations and resources (security breach).

 Provide an audit carried out after the security breach that certifies the correct operation and configuration of the information system for the purpose of prevent undue exposure to outside third parties of data resources as well as a new risk analysis.

THIRD: NOTIFY this resolution to IKATZ, S.A., with NIF A01043652 and with address at C/ Arkatxa 1, Pabellón 4 (Pol. Industrial Uritiasolo), 01006 Vitorial-Gasteiz, Araba (Alava).

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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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