 File No.: PS/00166/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On February 3, 2021,

TRADE UNION ALTERNATIVE

PRIVATE SECURITY WORKERS (hereinafter, the complaining party),

filed a claim with the Spanish Agency for Data Protection, against

EULEN SECURITY, S.A. with NIF A28369395 (hereinafter, the claimed party).

The complaining party states that the entity complained against is disclosing the number of

DNI of the personnel who perform their functions in the offices of the Center of

Training of Los Cármenes (Employment Agency of the Madrid City Council) to

through the informative note on the use of the workplace clothing, which have been

to sign the employees.

The affected party, who has raised the claim on behalf of the ALTERNATIVA union

SINDICAL, as a union delegate, considers that data such as the DNI can

be used by others fraudulently or for other purposes than to

which is being treated, so it should not be exposed in this way, in view of

other workers of the company or the client (e.g. receptionists, cleaning, other

companions...).

It states that not only is your consent not being requested for said treatment,

but, in addition, they are being pressured to obtain the document already signed.

Provides an image of the informative note in question and a screenshot of the emails

of the claimant with the Service Manager of the company, where the latter

request the aforementioned note already signed.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the respondent, so that

proceed to its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

On March 31, this Agency received a written response, although the

The company does not clarify the reason for exposing the complete ID number of the employees

that they have to sign the sheet with the new conditions, allowing each of them

have access to the identifier of those who have signed before, in a document whose

final custody corresponds to the company that is collecting the information.

Likewise, it states that it is a communication of data protected in the relationship

contractual, that the document was temporarily in an area

restricted with the proper security measures to which only the

security personnel and that as a result of this claim, the

possibility that, in the event that it is necessary to publish a D.N.I, compliance with

the seventh additional provision of Organic Law 3/2018, of December 5, of

Protection of Personal Data and Guarantee of Digital Rights.

THIRD: On April 8, 2021, in accordance with article 65 of the

LOPDGDD, the Director of the Spanish Data Protection Agency agreed

admit for processing the claim filed by the claimant against the respondent.

FOURTH: On August 18, 2021, the Director of the Spanish Agency for Data Protection agreed to initiate a sanctioning procedure against the claimed party, for the alleged infringement of article 5.1.f) of the RGPD and article 32 of the RGPD, typified in article 83.5 and 83.4 of the RGPD, respectively.

FIFTH: Once the initiation agreement was notified, the claimed party submitted a written allegations in which, in summary, it stated that the incident was caused by a human error motivated mainly by the urgency in notifying the measures that should be adopted after eliminating the ventilation system, which has been a accidental and fortuitous course that has been framed within the internal sphere of the company, that the volume of data and the type of data affected has been minimum, which has not had any consequences for the claimant or for the employees of the service, that the data was only visible for a short period of time and that preventive measures have been taken to avoid this type of case, and requests the filing of the claim filed and, failing that, the dismissal of the present sanctioning file

SIXTH: On December 9, 2021, a resolution proposal was formulated, proposing:

<<That the Director of the Spanish Data Protection Agency sanction EULEN SEGURIDAD S.A., with NIF A28369395, for an infringement of article 5.1.f) of the RGPD and article 32 of the RGPD, typified in article 83.5 of the RGPD, with a fine of THREE THOUSAND EUROS (€3,000)>>

SEVENTH: On December 23, 2021, the respondent files a written statement allegations to the Motion for a resolution, in which, in summary, it states that, in case of knowledge, all the necessary actions would have been taken and activated the corresponding procedures to minimize the incidence and implement actions

corrective measures to it, that the present incident has not caused a loss of

disposition and control over personal data, since they were

perfectly located and within a secure environment, which has not involved a

risk to the rights of those affected to the extent that there was limited access

and temporary to basic personal data (they do not belong to categories

special data), within a work environment and trust and has not involved

no harm to those affected after a year, states that they have been applied

security measures according to the defined risks and that the employee

included the identity document by mistake, skipping internal procedures,

given the urgency of the case and the situation derived from COVID, for which it requests the

file of the claim filed on the day.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: On February 3, 2021, the claimant filed a claim

before the Spanish Data Protection Agency, stating that the entity

claimed was disclosing the ID number of the company's employees to

through an informative note that they had to sign.

SECOND: Checking the documentation provided and that it is incorporated

to the file, it is clear that third parties had unauthorized access to data of

personal character of company employees.

THIRD: The claimed party acknowledges that the document was in a

in a restricted area with due security measures to which only

security personnel had access and that, as a result of this complaint,

assessing the possibility that, in the event that it is necessary to publish a D.N.I,

the seventh additional provision of the Organic Law 3/2018, of 5 of

December, Protection of Personal Data and Guarantee of Digital Rights.

FOURTH: Currently, the respondent states that he has proceeded to implement the

adequate corrective measures to avoid the repetition of similar events in the

future.

FOUNDATIONS OF LAW

FIRST: In accordance with the powers that article 58.2 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), grants

each control authority and as established in articles 47 and 48.1 of the Law

Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of

digital rights (hereinafter, 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 Agency for Data Protection will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures.”

SECOND: Regarding the allegations presented to the Resolution Proposal, it is

should point out the following:

In the first place, from the facts proven in this proceeding, it can be deduced that the

visualization of personal data by third parties, allow

verify that the claimed party has not been able to guarantee adequate security in the

treatment of the personal data of the employees of the company, incurring by

this in the violation of article 5.1 f) of the RGPD, which governs the principles of integrity

and confidentiality of personal data, as well as the proactive responsibility of the

data controller to demonstrate compliance.

In the specific case under examination, the claimed facts are specified in the

distribution of an informative note among the employees, which they had to fill in with their

name, surnames, DNI and signature, allowing access between them, to the identifier of the

that they had signed before. In other words, the company was authorized to treat

internally and know certain information, but was not entitled to

transfer it to third parties.

In this sense, it should be noted that the DNI together with the name and surname of the person

It is considered personal data, both by the RGPD and by the LOPDGDD. Y

it is so because through this, a person could be identified and being a data

personal, the same protection measures must be applied as for other data

personal.

Both the RGPD and the LOPDGDD aim to guarantee the rights

rights of natural persons and, in particular, their right to the protection of

personal data protected by article 18 of the Constitution. Thus,

any personal data that the company may process in relation to the workers,

is protected by the personal data protection regulations through the

application of a series of principles and guarantees that are required in relation to

any treatment that is carried out.

Secondly, as regards the argument that the incident has not led to a

loss of disposal and control over personal data, since they are

were perfectly located and within a secure environment, which has not

involved a risk to the rights of those affected to the extent that there was a

limited and temporary access to basic personal data (not belonging to

special categories of data), within a work environment and trust and has not

assumed no harm to those affected after one year, it is not a cause of

sufficient justification or exoneration, since those affected have been

devoid of control over your personal data.

In this case, the Internet search, for example, of the name, surnames of any of the

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

by 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.

The fact that it was an employee who mistakenly included the identity document,

skipping internal procedures, given the urgency of the case and the situation

derived from COVID, it should be noted that security measures must be adopted

in attention to each and every one of the risks present in a data processing of

personal character, including among them, the human factor. This risk must be

taken into account by the controller who, based on this, must

establish the necessary technical and organizational measures to prevent the loss of

control of the data by the data controller and, therefore, by the

the holders of the data that provided them.

Consequently, the allegations must be dismissed, meaning that the

arguments presented do not distort the essential content of the infraction that

declared to have been committed, nor do they imply sufficient cause for justification or exculpation.

THIRD: Article 5.1.f) of the RGPD, Principles related to treatment, establishes the

Next:

"1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational ("integrity and confidentiality").

Article 5 of the LOPDGDD, Duty of confidentiality, states the following:

"1. Those responsible and in charge of data processing, as well as all

people who intervene in any phase of this will be subject to the duty of

confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary to the

duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will be maintained even when

the relationship between the obligor and the person in charge or in charge of the transaction had ended.

treatment”.

The documentation in the file proves that the claimed party violated the

article 5 “Principles related to treatment” of the RGPD, section 1.f), in relation to

Article 5 “Duty of confidentiality” of the LOPGDD, when disclosing information and data

of a personal nature to third parties.

This duty of confidentiality, previously the duty of secrecy, must be understood

whose purpose is to avoid those leaks of data not consented to by the users.

holders of these This is an obligation that falls to the person in charge and in charge

treatment, as well as anyone who intervenes in any phase of the

treatment; and that it is complementary to the duty of professional secrecy.

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

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 for the guarantees of the rights and freedoms of the interested parties:

“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, as a consequence of a failure to implement measures

technical and organizational has caused access by unauthorized third parties to the

personal data of company employees.

From the actions carried out, there is evidence of the existence of reasonable indications and

enough that the security measures, both of a technical nature and

organizations, with which the claimed party had in relation to the data that

undergoing treatment, were not adequate at the time of the gap of

security, thereby violating article 32 of the RGPD.

The consequence of this lack of security measures was exposure to third parties

outside of the personal data of company employees. That is, those affected

have been deprived of control over their personal data.

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

example, of the name, surnames, DNI or email of any of those affected

can offer results that combining them with those now accessed by third parties,

allow us access to other applications of those affected or the creation of profiles

of personality, which do not have to have been consented to by their owner.

This possibility represents an added risk that must be assessed in the study of

risk management and that increases the demand for the degree of protection in relation to

the security and safeguarding of the integrity and confidentiality of these data.

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

establish the necessary technical and organizational measures to prevent the loss of

control of the data by the data controller and, therefore, by the data controllers.

holders of the data that provided them.

FIFTH: Article 83.5 of the RGPD, provides the following:

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

paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or,

in the case of a company, an amount equivalent to a maximum of 4% of the

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

the largest amount:

a)

basic principles for treatment, including conditions for con-

sentiment under articles 5, 6, 7 and 9;”

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what

following: "The acts and behaviors referred to in the

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

are contrary to this organic law.”

For the purposes of the limitation period for infractions, article 72 of the LOPDGDD,

under the rubric of infractions considered very serious, it establishes the following: “1. In

Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

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:

(…)

Yo)

The violation of the duty of confidentiality established in article 5 of

this organic law.

The violation of article 32 RGPD is typified in article 83.4.a) of the

cited RGPD in the following terms:

"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 to 39, 42 and 43."

(…)

For the purposes of the limitation period for infractions, article 73 of the LOPDGDD,

establishes under the heading "Infringements considered serious", the following:

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

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:

(…)

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.

In the present case, the infringing circumstances provided for in article

83.5 and 83.4 of the RGPD transcribed above.

SIXTH: In order to determine the administrative fine to be imposed, the

provisions of articles 83.1 and 83.2 of the RGPD, precepts that indicate:

"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 the

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

nature, scope or purpose of the processing operation in question, as well as the number

number of interested parties affected and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to pa-

allocate 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,

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

e) any previous infringement committed by the person in charge or the person in charge of the treatment;

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

infringement and mitigate the possible adverse effects of the infringement;

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

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

whether the person in charge or the person in charge notified the infringement and, if so, to what extent.

gives;

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

previously 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 to certification mechanisms

approvals approved in accordance with article 42,

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

such as financial benefits obtained or losses avoided, directly or indirectly.

mind, through infraction."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

"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 graduation criteria

established in section 2 of the aforementioned article.

2. In accordance with the provisions of article 83.2.k) of 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/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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 precepts transcribed, in order to set the amount of the penalty for

infringement of article 5.1 f) and 32 of the RGPD, to the party claimed as responsible for

the aforementioned infractions, the fine must be graduated taking into account:

-The intentionality or negligence appreciated in the infringement: in the present case,

There is evidence of gross negligence in conduct when exposing personal data of

employees of the company to outside third parties who had unauthorized access to

said data.

-The linking of the activity of the offender with the performance of data processing

personal, since the business activity of the defendant requires a continuous

processing of personal data of both clients and third parties, since

It is one of the largest companies in the country in its business or activity sector.

At the same time, the following criteria concur as mitigating factors:

Article 83.2.c) RGPD: any measure taken by the person responsible or in charge of the

treatment to alleviate the damages suffered by the interested parties

Article 83.2.h) RGPD: 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, to what extent.

In the present case, the respondent has informed this Agency of the circumstances

in which the incident that led to the claim occurred, as well as the measures

to adopt in order to prevent events such as the one claimed from occurring again in the future.

turo.

Article 83.2 k) RGPD: any other aggravating or mitigating factor applicable to the cir-

circumstances of the case. Likewise, it is considered that the response has been reasonable, re-

knowing the facts, not having evidence of other claims by

affected people.

Considering the exposed factors, the valuation that reaches the amount of the fine

is €2,000 for violation of article 5.1 f) of the RGPD, regarding the violation of the

principle of confidentiality and €1,000 for infringement of article 32 of the aforementioned

RGPD, regarding the security of the processing of personal data.

SEVENTH: Establishes Law 40/2015, of October 1, on the Legal Regime of the Sector Public, in Chapter III on the "Principles of the power to sanction", in the Article 28 under the heading "Responsibility", the following:

"1. They may only be sanctioned for acts constituting an administrative infraction. natural and legal persons, as well as, when a Law recognizes their capacity to to act, the affected groups, the unions and entities without legal personality and the independent or autonomous estates, which are responsible for them title of fraud or guilt."

Lack of diligence in implementing appropriate security measures with the consequence of breaching the principle of confidentiality constitutes the element of guilt.

EIGHTH: Article 70.1 of the LOPDGDD indicates the responsible subjects.

"1. They are subject to the sanctioning regime established in Regulation (EU) 2016/679 and in this organic law:

a) Those responsible for the treatments."

Of the evidence that is available according to the facts proven in the pre-present sanctioning procedure, the infraction of articles 32 and 5.1.f) of the RGPD, in the terms described above.

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of the sanctions whose existence has been proven, the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE EULEN SEGURIDAD S.A., with NIF A28369395, for a infringement of article 5.1.f) of the RGPD, typified in art. 83.5 of the RGPD, and for a infringement of article 32 of the RGPD, typified in article 83.4 of the RGPD, respectively, a fine of €2,000 (two thousand euros) and a fine of €1,000 (one thousand euros). This makes a total of €3,000 (three thousand euros).

SECOND: NOTIFY this resolution to EULEN SEGURIDAD S.A.

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case

Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following month or immediately after, and if

between the 16th and last day of each month, both inclusive, the payment term

It will be until the 5th of the second following month or immediately after.

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 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 month from
counting 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,
may provisionally suspend the firm resolution in administrative proceedings if the
The interested party expresses his intention to file a contentious-administrative appeal.
If this is the case, the interested party must formally communicate this fact by
writing addressed to the Spanish Agency for Data Protection, presenting it through
Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-
web/], or through any of the other registers provided for in art. 16.4 of the
aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the
documentation proving the effective filing of the contentious appeal-
administrative. If the Agency was not aware of the filing of the appeal
contentious-administrative within a period of two months from the day following the
notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-270122

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es