 File No.: EXP202100091

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: The MUNICIPAL POLICE UNION UNION (hereinafter the

claimant), with NIF P2807900B dated 06/10/2021 filed a claim with the

Spanish Data Protection Agency. The claim is directed against

MADRID CITY COUNCIL with NIF P2807900B (hereinafter the claimant). The

The reasons on which the claim is based are the following: the claimant states that the

05/06/2021 *** POSITION 1, sent an order to the rest of the police departments

hierarchical in an internal note in which personal data was requested; of the aforementioned note

It can be deduced that the intention of ***PUESTO.1 was to transfer the personal data and the

mobile phone numbers to a company (***COMPANY.1), which has the practice

customary to store them on a server located in a third country.

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

December, Protection of Personal Data and guarantee of digital rights (in

forward LOPDGDD), on 07/02/2021 the claim was transferred to the party

claimed, so that it proceeds to its analysis and informs this Agency within the term

of one month, of the actions carried out to adapt to the foreseen requirements

in the data protection regulations.

On 07/22/2021, this Agency received a written response indicating that the

said note or internal order, as it expresses, responds to an action

generated for all Madrid City Council staff with the aim of

guarantee the security of communications, it is not therefore, as stated in the

writing of the Union, a collection of data with the intention of transferring them to

a company, but rather, an action legitimized by the mere fact of the

fulfillment of a mission carried out in the public interest and in the exercise of powers

rights conferred on the person responsible for the treatment, among others, to guarantee the good

operation of public services.

THIRD: On 07/27/2021 the Director of the Spanish Protection Agency

de Datos agreed to admit the claim presented by the claimant for processing.

FOURTH: On 02/02/2022, the Director of the Spanish Protection Agency

of Data agreed to start a sanctioning procedure against the person claimed by the alleged

infringement of article 6.1 of the GDPR, typified in article 83.5.a) of the aforementioned GDPR.

FIFTH: Once the start agreement was notified, the claimant on 02/16/2022 presented

brief of allegations stating in summary the following:

- There is no illegal data processing in any way; the internal note is

precisely the one that gives transparency to the purpose of the use of the data that

are requested, explaining the origin that gives rise to the request, the object, the purpose

functional and operational purpose of the treatment.

- It is not possible to speak of illegality of the treatment, as expressed in the Agreement of

beginning, since article 6 of the GDPR makes explicit in point 1. c) that it becomes lawful

processing if it is necessary for compliance with a legal obligation

applicable to the controller and the aforementioned obligation is supported by the

obligation to provide the public security service that the Police Corps

Municipal must lend to citizens and that is based on the Agreement of the Board of

Government of June 27, 2019.

- It is also not possible to speak of contract execution and, much less, towards the Management

General Security, since it does not create any contract related to the

course that concerns us, but rather an adaptation to new technologies,

initiated for the entire City Council (...), whose mode of use requires access

secured through the identification method of the worker through the number of

mobile phone.

- It is not possible not to provide the mobile phone number of the officials who carry out their

tasks in the functional field that requires computer tools, since

It would mean a stoppage of the service (...) whose missions are included in the

public interest and within the constitutional framework of protecting the free exercise of rights and

freedoms and guarantee citizen security.

- The report provided specifies that ***COMPANY.1 is an entity in charge of

treatment through contracting file with the aim of modernizing the

workspace of the public employee, establishing the custom agreements of

treatment, having given his approval the Data Protection Delegate of the

City Council, not in the case of a transfer of data to ***COMPANY.1, but a

custom treatment contract for the performance of certain services.

- The consent has been provided (...), which expresses the explicit consent

offered by them through a direct action, not being able to express the

claimant that the telephone was obtained without the knowledge of those affected due to

the open publicity of the internal note and the response in order to proceed to the

technological updates.

SIXTH: On 08/10/2022, it was agreed to open an internship period for

tests, remembering the following:

- Deem reproduced for evidentiary purposes the claims filed and

its documentation, the documents obtained and generated that are part

of procedure E/07594/2021.

- Consider reproduced for evidentiary purposes, the allegations to the agreement of

initiation of the referenced disciplinary procedure, presented by the

claimed, and the documentation that accompanies them.

- Ask the defendant for a Contract signed with ***COMPANY.1 "(...)".

On 08/18 and 19/2022, the defendant responded to the practical test

whose content is in the file.

SEVENTH: On 09/29/2022, a Resolution Proposal was issued in the sense

that the Director of the Spanish Data Protection Agency sanctioned

to the person claimed for infringement of article 6.1 of the GDPR, typified in the

Article 83.5.a) of the aforementioned Regulation with a warning penalty. Also, it

attached Annex containing the list of the documents contained in the

file in order to obtain a copy of those deemed appropriate.

The representation of the defendant presented on 10/17/2022 a brief in which it alleged in

summary: that in the process of modernization and adaptation to new technologies

undertaken by the defendant made it necessary to incorporate security systems that

eliminate external threats; that the ENS determines that the person responsible for

security will establish the security requirements of the information and services,

taking charge of developing the specific way to implement this security by itself or

through contracted third parties and that the strategy will be based on the ENS guides (...),

as well as several CCN guides (...) being for this reason necessary a number of

mobile phone to which to send notifications for each access and authorization for

register said number for this use; that by means of an Agreement the policy of

security of the information of the defendant and his agencies, (...).

EIGHTH: Of the actions carried out in this procedure, there have been

the following accredited:

PROVEN FACTS

FIRST. On 02/23/2021 it has entry into the Spanish Agency for the Protection of

Written information from the claimant stating that on 05/06/2021 *** POSITION 1, he sent the

other police departments a hierarchical order requesting personal data

(number, mobile phone), deducing that the intention was to transfer the data

personal and mobile phone numbers to a company (***COMPANY.1), which

has the usual practice of storing them on a server located in a third country.

SECOND. There is an Internal Note of 05/06/2021 stating that with

reason for mail migration (...), shared mailboxes are created in order to

guarantee the security of communications, requesting to fill in the Excel that is

attached with the mailboxes that should remain active; noting that "it should

keep the following in mind:

1. Shared mailbox: these are the generic email accounts that are used.

2. For each generic account, indicate the Responsible with Name, Surname and

Mobile phone.

3. The person in charge must assign Authorized Persons with Name, Surname and

Mobile phone.

The mobile phone request to authorized persons is defined as

consequence of the security requirement presented by said software, which uses

for access to the mailbox the introduction of a code that is sent by message

to the user's mobile phone, as a means of verifying their identity, means

similar to that used in banks.

It has already been carried out in all the dependencies that have their headquarters in the

Headquarters of the Corps, now extending to the rest.

(…)”

THIRD. There is evidence of an appeal filed against the previous brief (...) of

05/12/2021.

ROOM. There is a written response from the defendant indicating the inadmissibility of

the filing of the appeal as there is no administrative act subject to appeal of

in accordance with article 112.1 of the LPACAP; also points out that the aforementioned note

responds to an action generated for all personnel with the aim of guaranteeing the

security of communications, legitimized action for the fulfillment of a mission

carried out in the public interest and in the exercise of public powers vested in the

responsible for the treatment and guarantee the proper functioning of the services

public; that the treatment affected by this action corresponds to (...); that the note

has been transmitted according to regulations under the figure of the regulatory conduit, since

it is an order and that it contains that in order to access the

work items such as email through the shared mailbox,

requires a personal security code that is transmitted through the

mobile phone, which guarantees both individualized and authorized access, as well as, in its

case, part of the secrecy of communications.

FIFTH. The defendant in writing of 07/22/021 responded to the requirement of the AEPD in the same sense indicated in the previous fact.

SIXTH. It is provided by the defendant Contract signed with UTE ACCENTURE-SCC "(…).

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), grants each control authority and as established in articles 47 and 48.1 of the Law Organic 3/2018, of December 5, 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 Data Protection Agency will be governed by the provisions of Regulation (EU) 2016/679, in this organic law, for the regulatory provisions dictated in its development and, as soon as they are not contradict, on a subsidiary basis, by the general rules on the administrative procedures."

The facts denounced are materialized in the treatment of data by the

claimed without legitimizing basis and their assignment to a company that stores them in a

server located in a third country, which could imply the violation of the

regulations on data protection.

II

Article 5 of the GDPR deals with the principles that must govern the

processing of personal data. The aforementioned precept provides that:

"1. Personal data will be:

a) Treated in a lawful, loyal and transparent manner with the interested party;

(…)"

Said treatment could constitute a violation of article 6, Lawfulness

of the treatment, of the GDPR in its point 1 establishes that:

"1. Processing will only be lawful if at least one of the following is fulfilled

conditions:

a) the interested party gave his consent for the processing of his data

personal for one or more specific purposes;

b) the processing is necessary for the performance of a contract in which the

interested party or for the application at the request of this of measures

pre-contractual;

c) the processing is necessary for compliance with a legal obligation

applicable to the data controller;

d) the processing is necessary to protect vital interests of the data subject or

of another physical person;

e) the treatment is necessary for the fulfillment of a mission carried out in

public interest or in the exercise of public powers conferred on the person responsible

of the treatment;

f) the processing is necessary for the satisfaction of legitimate interests

pursued by the data controller or by a third party, provided that

such interests are not overridden by the interests or the rights and freedoms

of the interested party that require the protection of personal data,

in particular when the interested party is a child.

The provisions of letter f) of the first paragraph shall not apply to the

treatment carried out by public authorities in the exercise of their functions.

(…)

3. The basis of the treatment indicated in section 1, letters c) and e), must be

established by:

a) Union law, or

b) the law of the Member States that applies to the person responsible for the

treatment.

The purpose of the treatment must be determined in said legal basis

or, in relation to the treatment referred to in section 1, letter e), it will be necessary

for the fulfillment of a mission carried out in the public interest or in the exercise of

Public powers conferred on the data controller. This legal basis may

contain specific provisions to adapt the application of rules of this

Regulation, among others: the general conditions that govern the legality of the treatment

by the person in charge; the types of data subject to processing; the interested

affected; the entities to which personal data may be communicated and the purposes

of such communication; purpose limitation; the storage periods of the

data, as well as the operations and processing procedures, including the

measures to ensure lawful and equitable treatment, such as those relating to other

specific treatment situations under chapter IX. Union Law

or of the Member States will fulfill an objective of public interest and will be proportional

to the legitimate end pursued.

(…)”

On the other hand, article 4 of the GDPR, Definitions, in its sections 1, 2 and 11,

notes that:

“1) “personal data” means any information about an identified natural person

or identifiable ("the data subject"); Any identifiable natural person shall be considered

person whose identity can be determined, directly or indirectly, in particular

by means of an identifier, such as a name, an identification number,

location data, an online identifier or one or more elements of the

physical, physiological, genetic, psychological, economic, cultural or social identity of said

person;

"2) "processing": any operation or set of operations carried out

on personal data or sets of personal data, either by procedures

automated or not, such as the collection, registration, organization, structuring,

conservation, adaptation or modification, extraction, consultation, use,

communication by transmission, diffusion or any other form of authorization of

access, collation or interconnection, limitation, deletion or destruction;

"11) "consent of the interested party": any manifestation of free will,

specific, informed and unequivocal for which the interested party accepts, either through

a statement or a clear affirmative action, the processing of personal data that

concern him."

Also article 6, Treatment based on the consent of the affected party,

of the new Organic Law 3/2018, of December 5, on Data Protection

Personal rights and guarantee of digital rights (hereinafter LOPDGDD), points out

that:

"1. In accordance with the provisions of article 4.11 of Regulation (EU)

2016/679, the consent of the affected party is understood as any expression of will

free, specific, informed and unequivocal for which he accepts, either through a

declaration or a clear affirmative action, the processing of personal data that

concern.

2. When it is intended to base the processing of data on consent

of the affected party for a plurality of purposes, it will be necessary for it to be clearly

specific and unequivocal that said consent is granted for all of them.

3. The execution of the contract may not be made subject to the fact that the affected party consents to the

processing of personal data for purposes unrelated to the

maintenance, development or control of the contractual relationship".

1. The defendant is accused of a violation of article 6.1 of the GDPR, precept

that lists the different bases or legal foundations on which the

processing of personal data, being the concurrence of any of them a condition

necessary to respect the principle of legality provided for in article 5.1.a) of the GDPR.

II

In accordance with the provisions of article 6.1 of the GDPR, in addition to the

consent, there are other possible bases that legitimize the processing of data without

need to have the authorization of its owner, in particular, when it is

necessary for the execution of a contract in which the affected party is a party or for the

application, at his request, of pre-contractual measures, or when necessary

for the satisfaction of legitimate interests pursued by the person in charge of the

treatment or by a third party, provided that such interests do not prevail

interests or the fundamental rights and freedoms of the data subject that require the

protection of such data. Treatment is also considered lawful when it is

necessary for compliance with a legal obligation applicable to the person responsible for the

treatment, to protect vital interests of the data subject or of another natural person or to

the fulfillment of a mission carried out in the public interest or in the exercise of powers

public rights conferred on the data controller.

(…)

And in that second allegation, he states that "It is not possible to speak of illegality

of the treatment, as expressed in the Agreement of initiation referring to the illegality of the

treatment either based on consent, or on the necessity of a contract, all

time that the same article 6 of the RGPD explicit on the one hand in point 1 section c)

that the treatment becomes lawful if it is necessary for the fulfillment of a

legal obligation applicable to the data controller; said obligation comes

based on the obligation to provide a public security service that the

Municipal Police Corps…

2. The fundamental question that arises in the present is to determine if

one of the legitimizing bases of those collected in sections a) to f) is present

of the aforementioned precept, for the processing of personal data in relation to

the mobile phone of the police officers by the defendant.

It is obvious, in light of what is alleged by the defendant, that these are not the

listed in letters a) of article 6.1 of the GDPR, to which must be added that

The standard itself excludes the possibility that the treatments carried out by the

public authorities in the exercise of their functions may have as a legal basis

of said treatment the letter f) of article 6.1 GDPR, that is, the legitimate interest and,

In addition, we are not in the special situation defined in letter d), either.

since we are not dealing with a treatment to protect an essential interest for the

life of the interested parties.

Therefore, it should be noted that the legal bases that could legitimize

supposedly the treatment of data by the City Council are mainly

two: the need for processing to comply with a legal obligation

applicable to the data controller defined in letter c), or the need for the

processing for the fulfillment of a task carried out in the public interest or in the

exercise of public powers conferred on the data controller, defined in the

letter e).

In this regard, the LOPDGDD introduces article 8, relating to the "Treatment

of data due to legal obligation, public interest or exercise of public powers", which

clarifies when the processing of personal data may be considered based on the

compliance with a legal obligation enforceable to the person in charge, in the terms provided

in article 6.1.c) of the GDPR.

Thus, it indicates that the processing of personal data can only be considered

based on compliance with a legal obligation enforceable to the person in charge when so

provided by a rule of European Union Law or a rule with the force of law.

These rules will be responsible for determining the general conditions of the
treatment and the types of data object of the same, as well as the transfers that proceed
as a consequence of compliance with the legal obligation. Said norm may
also impose special conditions to the treatment, such as the adoption of
additional security measures or others established in chapter IV of the GDPR.

On the other hand, and regarding the processing of personal data based on the
performance of a mission carried out in the public interest or in the exercise of powers
conferred to the person in charge and in the terms provided in article 6.1 e) of the
GDPR, it will only be legitimate when it derives from a competence attributed by a
regulation with force of law.

3. The recipients of the processing carried out by the claimant, such as
Public administration, whether simple citizens or public employees, responds to the
GDPR definition of data controller as “public authority, service or
another body" and, therefore, it will be obliged to determine "the purposes and means of the
treatment” (article 4 7 of the GDPR). Precisely for this reason, the City Council in this
case, will be responsible for compliance with the principles that are projected on the
right to data protection, but also able to demonstrate compliance
(article 5.2 GDPR).

It is true that in the management of their human resources, the Administrations
They usually make use of the data of the people in their charge. We can confirm that the
Municipalities have the name and surname, the ID number, etc.

In the present case, it is disputed whether with respect to specific personal data,

How is the private mobile phone number, can it be treated? or for him

Otherwise, can its processing be considered unlawful, excessive and unnecessary?

In principle, the bases of the legality that the defendant could use for the

processing of personal data of police officers are specified in the

art. 6.1 section c) and e).

And indeed, the defendant in writing of 02/06/2022 has alleged as a basis

legitimizing the treatment contained in section c) of article 6.1. GDPR

by stating that "... processing becomes lawful if it is necessary for the

compliance with a legal obligation applicable to the data controller…"

The defendant manifests in his writing said legal obligation is supported

in providing the public security service whose competence is attributed the

Police in accordance with the rules that attribute it.

In this sense, Organic Law 2/1986, of March 13, on Forces and

State Security Corps (hereinafter LOFCS). Security Forces

of the State are divided into three administrative levels (national, regional and

local).

Article 11 of the LOFCS establishes that these units have the mission

protect the free exercise of rights and freedoms and guarantee security

citizen by performing the following functions:

(…)

e) Maintain and restore, where appropriate, public order and safety.

(…)”

Secondly, Law 7/1985, of April 2, regulating the Bases of the

Local Regime (LBRL), in its article 25 establishes that:

"1. The Municipality, for the management of its interests and within the scope of its

competencies, can promote activities and provide public services that

contribute to satisfying the needs and aspirations of the neighboring community in

the terms provided in this article.

2. The Municipality will exercise in any case as its own powers, in the

terms of the legislation of the State and the Autonomous Communities, in which

following subjects:

(…)

f) Local police, civil protection, fire prevention and extinction.

(…)”

On the other hand, Law 1/2018, of February 22, on Police Coordination

Locales of the Community of Madrid (LCPLCM), in its article 1, Object, establishes

that:

"1. The purpose of this Law is to regulate the coordination functions of the

Local police forces in the territorial scope of the Community of Madrid of

in accordance with the powers attributed to it by Organic Law 2/1986, of 13 December

March, of Security Forces and Corps, the Statute of Autonomy and the legislation

local regime, as well as determine the principles, policies and instruments of the

regional public security, within the framework of current legislation”.

And with regard to the Madrid City Council, the Police Regulations

Municipal Council of Madrid (RPMAM), in its article 5, Missions and

functions, states among others:

"m) Carry out the functions of protection of citizen security in accordance with

with current legislation".

It should be noted that the defendant is bound by the principle of

legality so that it can only carry out what the legal system

legal expressly allows.

The cited standards contain a generic mandate addressed to the different

Public administrations, of which the Town Halls are a part, so that

act in their generic and functional scope in order to maintain security

public with the means at its disposal and achieve the mission of protecting the free

exercise of rights and freedoms and guarantee citizen security.

However, the data processing carried out cannot be protected by the

letter c) of article 6.1 of the GDPR already requires that this is necessary for the

compliance with a legal obligation applicable to the data controller, therefore

that a sensu contrario, if the treatment is not necessary for the fulfillment of said

obligation the processing becomes unlawful.

And none of the indicated norms contain any precept that determines

that said treatment is necessary for the fulfillment of the same, nor is it

contemplated in the LCPLCM and the RPMAM the personal data related to the

mobile phone number.

Thus, with regard to the Regulations for the Municipal Police Corps: neither

article 42, professional identification, article 45, personal file, article 143,

professional license, nor in article 144, Portfolio and police badge, contain reference or

any obligation to provide the mobile phone number, nor does it contain

in article 45, Registry, of the LCPLCM that establishes:

"1. The Registry of local police officers will depend on and be managed by the

Department competent in matters of coordination of local police. His

organization and operation will be regulated by law, respecting, in all

case, the regulations contained in Organic Law 15/1999, of December 13, of

Personal data protection.

2. The purpose of the Registry of local police officers is to provide, for the purposes

statistics, of a census of all the members that make up the police forces

local councils of the Community of Madrid, as well as the staff of the

Bodies that are created under the provisions of article 53.3 of the Organic Law

2/1986, of March 13, of Security Forces and Corps.

3. The Registry of local police officers is not public, and its access

will be restricted in the terms established by law.

4. In the Registry of local police officers, the personnel that integrates

the various local police forces of the Community of Madrid as well as the agents

auxiliaries whatever the name by which they are known, and where appropriate the

personnel of the bodies that are created under the provisions of article 53.3 of

Organic Law 2/1986, of March 13, on Security Forces and Bodies.

The registration must contain the name, surname, date and place of

birth, number of the National Identity Document and of the Personnel Registry

of the interested party in the corresponding town hall" (underlining corresponds to

the AEPD).

For its part, art. 6.3 of the GDPR indicates that "The purpose of the treatment

must be determined in said legal basis" and in the case examined the

activity carried out to which the processing of personal data is linked.

personal nature (...) is not related to the purposes of the police; the treatment

is determined by access to computer applications, access to the mailbox

shared by entering a code that is sent to the mobile phone

to verify the identity of the user, like any other official of the defendant,

within the process of modernization and adaptation to new technologies

undertaken by the claimed in its different services.

In the pleadings to the initiation agreement, the defendant himself states

that (...), whose mode of use requires secure access through the method

identification of the worker..." and the Internal Note of 05/06/2021 regarding mailboxes

shares is indicated in its third paragraph "It is an action generated to

the entire Madrid City Council, in order to guarantee the safety of the

communications,…"

And in the same contract signed with UTE ACCENTURE-SCC (...) it is indicated

that:" (…)".

Therefore, such activity cannot be legitimized in compliance with a

legal obligation but as the defendant points out in his brief in an adaptation to

the new technologies, (…).

Thus, being accredited that the defendant has processed the data of the number

agent mobile number being one of the elements or requirements demanded by the software

contracted, for access to the shared mailbox by entering a code

that is sent by message to the user's mobile, as a means of verification of

your identity without it being contemplated in any norm, cannot operate as a base

legitimizing the treatment the fulfillment of a legal obligation (letter c, of the

article 6.1 of the GDPR)

It is concluded from the foregoing that the processing of personal data of the

claimant who is being assessed in this disciplinary file does not

covered by none of the legal bases of article 6.1. GDPR. Violation of

article 6.1 of the RGPD that is subsumable in the sanctioning type of article 83.5.b) of the

GDPR.

4. Lastly, the claimant also alleged in his statement of claim that

the intention of the defendant was to transfer personal data (including the number of

mobile phone), to a company, ***COMPANY.1, whose usual practice is

store them on a server located in a third country.

However, such a manifestation cannot be shared, abstracted from

what is indicated in the previous grounds that the defendant does not have a basis

any legal authority to process the data of the mobile phone number.

The defendant has provided a copy of the contract entered into with UTE ACCENTURE

SCC, ***COMPANY.1, in which Annex XI called the Assignment Agreement of the

Treatment, the agreements reached are established, which in addition to having the

approval of the Data Protection Officer, is in accordance with the recommendations

and AEPD guidelines.

Recital 81 of the GDPR provides that the person in charge of the treatment must
provide sufficient guarantees in terms of expertise, reliability
and resources, with a view to the application of technical and organizational measures that comply with
the requirements of the Regulation, including the security of the treatment, as well as the
compliance with data protection regulations.

(81) To ensure compliance with the provisions of this
Regulations regarding the treatment carried out by the person in charge on behalf of the
responsible, the latter, when entrusting treatment activities to a manager, must
resort only to managers who offer sufficient guarantees, in particular in
in terms of expertise, reliability and resources, for the
application of technical and organizational measures that meet the requirements of the
this Regulation, including the security of the treatment. The accession of
entrusted to an approved code of conduct or certification mechanism
approved can serve as an element to demonstrate compliance with the
obligations on the part of the controller. Processing by a processor must be governed
by a contract or other legal act in accordance with the law of the Union or of the
Member States that links the person in charge with the controller, that establishes the object and the
duration of the treatment, the nature and purposes of the treatment, the type of data
personal and the categories of data subjects, taking into account the functions and
specific responsibilities of the processor in the context of the treatment to be
be carried out and the risk to the rights and freedoms of the interested party. He
controller and processor may choose to rely on an individual contract or on
standard contractual clauses adopted directly by the Commission or first
adopt a supervisory authority in accordance with the consistency mechanism and
later the Commission. Once the treatment has been completed on behalf of the
responsible, the person in charge must, at his choice, return or delete the data

personal data, unless the law of the Union or of the Member States applicable to the

person in charge of the treatment obliges to keep the data.

The contract signed with the successful bidder includes, of course, in the

section on data protection and confidentiality of information for

guarantee that the processing of personal data is in accordance with the

regulations in force. (...) (to this information ***COMPANY.1 should not access,

although we must not forget that she is the administrator of the service so she could have

data access).

The licensed ***COMPANY.1 solution has the (…).

In addition, the defendant has the requirements (...).

In the same way, in the allegations to the initiation agreement, it has been provided

certificate (...) on ***COMPANY.1.

Therefore, there is no transfer of personal data, but a custom contract of

treatment for the performance of certain services that apparently counts

with guarantees and sufficient security.

5. Regarding the email service, it is based on a

platform ***PLATFORM.1.

Annex III of the signed contract (...), indicates as a solution the migration of the

email and provide said service (...) (Royal Decree 3/2010) in force and

be in accordance with the regulations for the protection of personal data.

Likewise, it is pointed out that (...) who will determine, among the solutions of

authentication proposals, those that it considers most appropriate and the successful bidder will be implemented in the service.

In this sense, the mobile phone number is one of the elements or security requirements presented by the computer system or software, which you use to access to the shared mailbox the introduction of a code that is sent by message to the user's mobile phone, as a means of verifying their identity, similar to that used in banks.

The use of this double authentication factor is a method that confirms that a user is who they say they are by combining two different components and the method more widespread to access email accounts.

Implementing this method is an effective way to prevent attacks on sensitive information that may compromise personal data, in addition, of limiting the employee's reach to information through the use of devices and to become aware of the use and management of good security practices.

As well summarized by the National Institute of Cybersecurity (INCIBE) there are three forms or families of authentication: 1. Something you know (a password) 2. Something that you have (a certificate, a mobile phone, a key, etc.) 3. Something that you are (biometrics: fingerprint, face, iris, etc.).

The need to use two-factor authentication (something you know + something you have) is a very enforceable security check, making it difficult to possible impersonation of the identity of the legitimate user, since it adds another factor of identification in the access to the data stored in the instance (...), in such a way so that even if someone knew a user's password, they could not access the service by not being able to verify the code sent by SMS or by phone call.

However, in the present case the defendant uses as one of the elements to achieve this double authentication factor of personal data,

(...), for which it is not legitimized as previously accredited by not

none of the legitimizing bases of those collected in sections a) to f) concur

of article 6.1 of the GDPR that would allow the processing of personal data

staff.

However, (...) is not the only element that can be used to achieve

that double authentication factor, but as indicated by INCIBE they can be

used other elements or factors to achieve user identification (a

cryptographic card with a certificate of public employee, hardware or software, etc.).

The defendant himself has stated in his brief of 08/19/2022 that: "(...)".

The own mobile application ***APLICATION.1" can be used to

enter office 365 and receive the double authentication factor, (...).

IV.

The defendant in writing of 10/17/2022 presented allegations to the Proposal for

Resolution stating that the process of adaptation to new technologies makes

necessary to incorporate security systems that eliminate external threats from

in accordance with the general principles of action of the administrations

public, contained in Law 40/2015, norm that indicates that the ENS establishes the

security policy in the use of electronic means constituting the

basic principles and minimum requirements that guarantee information security

treated.

It should be noted that there is nothing to object to the alleged that in the process

modernization and adaptation of administrative services to the new

technologies it is necessary to adapt to new scenarios in order to achieve

a more efficient and effective administration, incorporating security systems

that abort the threats that may occur and in this sense the

allusion to article 156, National Interoperability Scheme and National Scheme

of Security, of Law 40/2015 is considered appropriate.

This same standard has extended the scope of application of the ENS to the entire

public sector, establishing in its article 3 the need for the administrations

relate to each other and to their bodies, public agencies and entities

linked or dependent through electronic means, so that

guarantee the interoperability and security of the systems and solutions adopted by

each of them and the protection of personal data, facilitating the provision of

services preferably by said means, indicating the ENS as the instrument

essential for the achievement of these objectives.

Also Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations, indicates among the rights of individuals

in their relations with public administrations provided for in article 13, h) the

regarding "The protection of personal data, and in particular the security and

confidentiality of the data contained in the files, systems and applications of

the Public Administrations".

Therefore, nothing has started so that the contract file formalized by

the defendant conveys the security strategy in accordance with the

principles, requirements and guidelines of the ENS and the CCN for the configuration of the products

***COMPANY.1, as well as the establishment of the double authentication factor

mandatory.

As previously indicated in Annex III of the signed contract (...), in

Consistent with what was indicated by the defendant in his allegations, it is indicated that:

“(…)”.

However, it is not the purpose of this proceeding to determine whether the defendant

in the process of modernization and adaptation to new technologies has adapted

its performance to the general principles of performance of public administrations,

contained in Law 40/2015; that in terms of safety in the use of

electronic means conforms to what is indicated in the ENS or the use of guides

ENS specific to ***COMPANY.1, as CCN guides for the configuration of

all ***COMPANY.1 Online products, as well as the double authentication factor

mandatory.

In the present case, what is sought to be determined is whether the defendant holds

legal authorization for the use of the controversial personal data, number

of mobile telephony, becoming an univocal and necessary element for access

as a means to verify identity and validate authentication; question is

that has not been distorted by the defendant in his allegations.

Likewise, it has been pointed out that compliance with the ENS for a MEDIUM level,

the controls “op.acc.5” and “op.acc.6” force the use of a second factor of

authentication to access corporate information and services.

V

Article 83.5 a) of the GDPR, considers that the infringement of "the principles

principles for treatment, including the conditions for consent under

of articles 5, 6, 7 and 9” is punishable.

On the other hand, the LOPDGDD in its article 72 indicates:

considered very serious:

“Infractions

1. Based on what is established in article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

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

particular, the following:

(…)

b) The processing of personal data without the concurrence of any of

the conditions of legality of the treatment established in article 6 of the

Regulation (EU) 2016/679.

(…)”

SAW

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

17/20

However, article 77 of the LOPDGDD, Regime applicable to certain

categories of controllers or processors, establishes the following:

"1. The regime established in this article will be applied to the treatments

for which they are responsible or in charge:

a) The constitutional bodies or those with constitutional relevance and the

institutions of the autonomous communities analogous to them.

b) The courts.

c) The General State Administration, the Administrations of the

autonomous communities and the entities that make up the Local Administration.

d) Public bodies and public law entities linked or

dependent on the Public Administrations.

e) The independent administrative authorities.

f) The Bank of Spain. g) Public law corporations when they are

purposes of the treatment are related to the exercise of powers of

public Law.

h) Public sector foundations.

i) Public Universities.

j) Consortiums.

k) The parliamentary groups of the Cortes Generales and the Assemblies

Autonomous legislatures, as well as the political groups of the Corporations

Local.

2. When the managers or managers listed in section 1

commit any of the offenses referred to in articles 72 to 74 of

this organic law, the competent data protection authority will issue

resolution sanctioning them with a warning. The resolution will establish

likewise, the measures that should be adopted to cease the conduct or to correct it.

the effects of the offense committed.

The resolution will be notified to the person in charge or in charge of the treatment, to the

body to which it depends hierarchically, if applicable, and to those affected who have

the condition of interested party, if applicable.

3. Without prejudice to what is established in the previous section, the authority of

data protection will also propose the initiation of disciplinary actions

when there is sufficient evidence to do so. In this case, the procedure and the

The sanctions to be applied will be those established in the legislation on the disciplinary regime.

or sanction that results from application.

Likewise, when the infractions are attributable to authorities and executives,

and the existence of technical reports or recommendations for treatment is accredited

that had not been duly attended to, in the resolution in which the

sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or regional Gazette that

corresponds.

4. The data protection authority must be informed of the

resolutions that fall in relation to the measures and actions to which they refer

the previous sections.

5. They will be communicated to the Ombudsman or, where appropriate, to the institutions

analogous of the autonomous communities the actions carried out and the

resolutions issued under this article.

6. When the competent authority is the Spanish Agency for the Protection of

Data, it will publish on its website with due separation the resolutions

referring to the entities of section 1 of this article, with express indication of the

identity of the person in charge or in charge of the treatment that had committed the

infringement.

When the competence corresponds to an autonomous protection authority

of data will be, in terms of the publicity of these resolutions, to what is available

its specific regulations."

In the present case, the present disciplinary procedure was opened in

based on the presumption that the defendant has violated the regulations on

protection of personal data, principle of legality of the data.

In accordance with the available evidence of such conduct

constitutes, on the part of the defendant, the infringement of the provisions of article 6.1 of the

GDPR.

This has been accredited when processing the personal data of the

police officers, mobile phone number, without stating that he had a database

legitimacy for it.

It should be noted that the GDPR, without prejudice to the provisions of its article 83,

contemplates in its article 77 the possibility of resorting to the sanction of warning and

correct the processing of personal data that does not conform to its forecasts,

when the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this law

organic.

Likewise, it is contemplated that in the resolution that is issued,

establish measures that should be adopted to stop the conduct, correct the

effects of the offense committed and its adequacy to the requirements

contemplated in article 6.1 of the GDPR, as well as the contribution of means

certifying compliance with the requirements.

It is necessary to point out that repeating the behavior revealed in the

claim and that is the cause of this procedure, as well as not informing

subsequently to this AEPD of the measures adopted to avoid incidents such as

indicated could give rise to the exercise of possible actions before the person in charge of the

treatment in order to effectively apply the measures that guarantee and

do not compromise the legality of the processing of personal data.

The corrective powers that the GDPR attributes to the AEPD as authority of

control are listed in article 58.2, sections a) to j).

VII

Article 83.5 of the GDPR establishes a sanction of an administrative fine (article

58.2.i) for the conducts that are typified therein, without prejudice to the fact that, as provided in the

article 83.2. of the GDPR, administrative fines can be imposed together with

other corrective measures provided for in article 58.2 of the GDPR.

Having confirmed the infringement, it is appropriate to impose on the person responsible the

adoption of appropriate measures to adjust its performance to the aforementioned regulations

in this act, in accordance with the provisions of the aforementioned article 58.2 d) of the GDPR,

according to which each control authority may “d) order the person in charge or in charge

of the processing that the processing operations comply with the provisions of the

this Regulation, where appropriate, in a certain way and within a certain

specified period”.

In the present case, the defendant is required so that within a period of one month

from the notification of this resolution:

- Accredit the adoption of measures so that they do not occur again

incidents such as the one that gave rise to the disciplinary procedure: the use of data

of a personal nature (...) without any legitimizing basis of those included in the

Article 6.1 of the GDPR and that the treatments carried out comply with the provisions

of this Regulation.

It is noted that not meeting the requirement can be considered as a

administrative offense in accordance with the provisions of the GDPR, classified as

infraction in its article 83.5 and 83.6, being able to motivate such conduct the opening of a

subsequent administrative sanctioning procedure.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE MADRID CITY COUNCIL, with NIF P2807900B, for a

infringement of article 6.1 of the GDPR, typified in article 83.5.a) of the GDPR, a

warning sanction.

SECOND: NOTIFY this resolution to the CITY COUNCIL OF MADRID.

THIRD: REQUEST the MADRID CITY COUNCIL, so that within a period of one

month from the notification of this resolution, accredit the adoption of measures to

that incidents such as the one that gave rise to the procedure do not occur again

sanctioning: the use of the mobile telephone number of the agents without attending

legitimizing basis any of those included in article 6.1 of the GDPR.

ROOM:

in accordance with the provisions of article 77.5 of the LOPDGDD.

COMMUNICATE this resolution to the Ombudsman, in

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

This Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process in accordance with art. 48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, interested parties may optionally file an appeal for reversal before the Director of the Spanish Data Protection Agency within a period of one 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 for in article 46.1 of the referred Law.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP, the firm resolution may be temporarily 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, presenting it 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 a period of two months from the day following the notification of this resolution, would terminate the injunction suspension

Electronic record of

through the

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es