 Procedure No.: PS/00509/2021

RESOLUTION OF PUNISHMENT PROCEDURE

Through an Agreement dated 01/03/22, the sanctioning procedure was initiated,

PS/0509/2021, instructed by the Spanish Data Protection Agency before the

GENERAL DIRECTORATE OF THE POLICE, (DGP), (hereinafter, "the party claimed"),

for alleged infringement of Regulation (EU) 2016/679, of the European Parliament and of the

Council, of 04/27/16, regarding the Protection of Natural Persons in what

regarding the Processing of Personal Data and the Free Circulation of these Data,

(RGPD) and Organic Law 3/2018, of December 5, on Data Protection

Personal and guarantee of digital rights, (LOPDGDD), and based on

the following:

BACKGROUND:

FIRST: On 06/02/21, this Agency received a letter from A.A.A.,

(hereinafter, "the complaining party"), in which, among others, it indicated the following:

“Last day 06/01/21 I was with a group of friends in the

confluence of General Aranaz and María Lombillo Madrid streets. Us

we were leaving a rally that had been convened

by the association "my safe neighborhood" and when we left the concentration,

various CNP callsigns proceeded to identify us and pass on our data

by the issuer for the purpose of carrying out the appropriate checks. One time

After completing the identification process and after checking the agents that everything

was correct, the agent proceeded to take pictures of our IDs with his

personal telephone, all this, despite being warned by those present that

we did not grant our consent for that photo taking of the DNI.

The agent herself told us that the photographs were being taken from

their personal telephone, since they do not have a staff telephone".

SECOND: Dated 07/01/21, in accordance with the provisions of article 65.4

of the LOPDGDD Law, by this Agency, said claim was transferred

to the DGP, so that it proceeded to its analysis and report, within a period of one month, on

what was stated in the statement of claim.

THIRD: On 07/23/21, the DGP sends this Agency a written response

to the request made, in which, among others, it indicated the following:

"The Organic Law 4/2015, of March 30, on the protection of the security

citizen, regulates in its article 16, the assumptions and the way in which the

Agents of the Security Forces and Bodies may request the

identification of people, enabling them to "carry out the checks

necessary on public roads or in the place where the

requirement, including the identification of persons whose face is not

Totally or partially visible due to the use of any type of garment or object that

cover, preventing or hindering the identification, when necessary to the

indicated effects", and must strictly respect "the principles of

proportionality, equal treatment and non-discrimination on the grounds of

birth, nationality, racial or ethnic origin, sex, religion or belief,

age, disability, sexual orientation or identity, opinion or any other

personal or social condition or circumstance.

In this sense, the aforementioned rule even provides that when it is not possible to

identification by any means, the agents could “require those who do not

could be identified to accompany them to the police stations

closest in which the adequate means are available for the

practice of this diligence, for the sole purpose of identification and for the

time strictly necessary.

In a context like the current one marked by the pandemic situation

international crisis caused by the coronavirus COVID-19, the practice of

identification procedures implies an increase in personal risk

for the performers. For this reason and in accordance with the advice disseminated

by the health authorities, the police officers take extreme measures of

self-protection of agents, also in the field of health and hygiene,

avoiding direct contact with the person identified and their belongings, looking for

asepsis environmental conditions and maintaining safety distances.

In this sense, the sole purpose of taking an image of the document

identity and with it to carry out the opportune verifications, was to avoid the

manipulation of this and keep the safety distance. In this way, the

photography is an exceptional way of proceeding at a time

marked by health and social circumstances of serious risk to health.

In order to know the specific circumstances in which the

facts described above, consultation was evacuated to the Superior Headquarters of Madrid.

The following conclusions are drawn from the report: - It has been found that the

The official took a single image of the National Identity Document of the

identified person, acting under article 16 of LO 4/2015, and with

the same effects and purpose as if the data had been taken from

manual way. - As stated in her Minutes-Report, the agent proceeded to

delete the document image once the purpose for which it was created has been fulfilled.

I take.

It should be noted that police action for criminal prevention and

maintenance of public order, the subject of this report, accommodated

specifically to the basic principles of action established in the

article 5 of the Organic Law 2/1986, of March 13, of Forces and Bodies

Security, as well as the current legislation on the protection of

data, specifically: • Directive (EU) 2016/680 of the European Parliament and of the

Council of April 27, 2016, regarding the protection of natural persons

with regard to the processing of personal data by the

competent authorities for purposes of prevention, investigation, detection or

prosecution of criminal offenses or execution of criminal sanctions, and

to the free movement of said data and by which the Framework Decision is repealed

2008/977/JAI of the Council, which has been transposed into Spanish law

through: • Organic Law 15/1999, of December 13, on Data Protection

of a Personal Nature, in force at the time of the events. • Organic Law

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

digital rights, which includes the following specifications. either

Unique derogatory provision. Regulatory repeal. 1. Without prejudice to

provided for in the fourteenth additional provision and in the transitory provision

fourth, the Organic Law 15/1999, of December 13, of

Personal data protection. Specifically, article 2.2

section a) of the aforementioned Organic Law 3/2018 in relation to article 2.2

section d) of Regulation (EU) 2016/679 of the European Parliament and the

Council, of April 27, 2016, regarding the protection of people

regarding the processing of your personal data and the free

circulation of these data expressly excludes the application of the Law

Organic 3/2018 to the processing of personal data "by the

competent authorities for the purposes of prevention, investigation, detection or

prosecution of criminal offenses, or execution of criminal sanctions,

including protection against threats to public safety and its

prevention".

It is participated that, from the Operational Deputy Directorate, will proceed to impart

instructions on the use of electronic devices by

police officers in operational actions, so as to ensure the

conformity of said actions to the regulations on the Protection of

Data".

FOURTH: Dated 10/18/21, in accordance with article 65 of the LPDGDD Law

by the Director of the Spanish Data Protection Agency, it is issued

agreement of admission of procedure of the presented claim, when appreciating possible

reasonable indications of a violation of the rules in the field of competences

of the Spanish Agency for Data Protection.

FIFTH: On 01/03/22, by the Board of Directors of the Spanish Agency for

Data Protection, a sanctioning procedure is initiated against the DGP, for violation

of the RGPD, when appreciating possible indications of infringement of 32.1 of the RGPD.

SIXTH: Notification of the initiation agreement to the DGP, the latter by means of a document dated

01/14/22 made, in summary, the following allegations:

“Regarding the identification procedure, the procedural agreement

sanctioning PS/00509/2021, performs an analysis of Organic Law 4/2015 of

March 30, protection of citizen security (hereinafter, LOPSC),

referring, firstly, to the preamble where it is stated that "...

empowers the competent authorities to agree on different actions

aimed at maintaining and, where appropriate, restoring tranquility

citizen in cases of public insecurity, precisely regulating the

budgets, purposes and requirements to carry out these procedures,

in accordance with the principles, among others, of proportionality, minimal interference

and non-discrimination…".

Reference is also made to articles 9, on the obligations and rights

of the holder of the National Identity Document and 16.1, in which

specify the cases in which the Security Forces and Bodies may

require the identification of persons ("When there are indications that they have

been able to participate in the commission of an offence, when it is necessary

to prevent a crime…"), and allusion is made to the strict respect for the principles

of proportionality, equal treatment and non-discrimination on the grounds of

birth, nationality, racial or ethnic origin, sex, religion or belief,

age, disability, sexual orientation or identity, opinion or any other

personal or social condition or circumstance, which must necessarily govern the

practice of identification diligence.

In relation to the provisions of Organic Law 4/2015 of March 30, the

General Directorate of the Police considers that the police action was carried out
with absolute respect for the principles contained in article 16.1 LOPSC
(proportionality, equal treatment and non-discrimination), being noteworthy
that there is no evidence that these extremes have been questioned by the claimant,
focusing the claim solely on the means used for the practice of
the identification. Article 16.2 LOPSC contemplates the use of any means
available to the agents that favors the act of identification.
In this sense, the official who carried out the identification procedure used
the means available to them, taking into account the circumstances
exceptional circumstances of the international pandemic context motivated by the
coronavirus SARS-CoV-2, in order to practice identification with a
that facilitated the intervention by minimizing interpersonal contact, which
as stated above, following the instructions of the authorities
healthcare in this regard.
Once the necessary checks were made, the images were deleted
without any trace of them remaining in any police file.
Likewise, it is considered that police action within the framework of
crime and maintenance of public order was specifically accommodated to the
basic principles of action established in article 5 of the Organic Law
2/1986, of March 13, on Security Forces and Bodies, as well as the
forecasts of the LOPSC itself.
SECOND.- The action that gives rise to this procedure consists
in the identification procedure that, as can be deduced from the articles
referenced above of the LOPSC, is part of the activity that, in terms of
prevention of criminal and administrative offenses, carried out by the Forces and
Security forces. It should be noted that the events that bring together

large concentrations of people, such as the one being analyzed,

They are usually taken advantage of by individuals or groups who, protected by the

multitude carry out criminal acts that must be prevented by the

FFCC Security to guarantee citizen security and the free development of

fundamental rights and public freedoms of other citizens.

THIRD.- The act that gives rise to this procedure consists of the

identification diligence carried out during the concentration

held in the Madrid district of San Blas, on June 1, 2021. The

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

guarantee of digital rights, alleged by the AEPD to initiate the

sanctioning procedure, expressly excludes from its scope of application

in its article 2.2 to the treatments excluded from the scope of application of the

General data protection regulation by its article 2.2, without prejudice to

the provisions of sections 3 and 4 of this article.

Article 2.2.d) of the RGPD regulates the scope of its material application, and

excludes the processing of personal data carried out by the

competent authorities for the purposes of prevention, investigation, detection or

prosecution of criminal offenses, or execution of criminal sanctions,

including protection against threats to public safety and its

prevention.

The processing of personal data by the competent authorities

for purposes of prevention, investigation, detection or prosecution of

criminal offenses or execution of criminal sanctions, at the time of

the facts that originate the present sanctioning procedure, continued

being subject to regulation by articles 23 and 24 of the Organic Law

15/1999, of December 13, on the Protection of Personal Data, in

under the provisions of Additional Provision 14 LPDGDD.

On the other hand, regarding the use of video cameras by the Forces and

Security Corps is concerned, the regulatory framework was given by the Law

Organic 4/1997, of August 4, which regulates the use of

video cameras by the Security Forces and Bodies in public places,

which, however, did not refer in its articles to any limitation or require

any authorization regarding the use of photographic cameras.

FOURTH.- The Agreement to initiate the sanctioning procedure, in its point IV,

analyzes the alleged excessive treatment of personal data of the

demonstrators, and alludes to an alleged violation of the provisions of article

5 LPDGDD, 1.c) specifies that "the processing of personal data must

be adequate, pertinent and limited to what is necessary in relation to the purposes

for which they are processed", known as the principle of data minimization.

FIFTH.- The Initial Agreement concludes that the known facts could

be constitutive of an infringement of article 32.1 RGPD: "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 probability and

variable seriousness for the rights and freedoms of natural persons, the

Responsible and the person in charge of the treatment will apply technical measures and

appropriate organizational arrangements to ensure a level of security adequate to the

risk, which, where appropriate, includes, among others: (...) b).- The ability to guarantee

the ongoing confidentiality, integrity, availability and resiliency of the

treatment systems and services", and in this case, where the agent performed

a photograph of the claimant's ID with his mobile phone for personal use,

does not guarantee at all what is stipulated in this article.

The aforementioned criterion is not shared by the Deputy Directorate of the

General Directorate of the Police, given the circumstances in which the

identification, given that the exposure of the document by its holder to the

agent and the consequent copying of the data by the latter, required

necessarily a temporary space of close contact wider than the

time required to take the photograph of the document, this being

last option, the one chosen by the acting official given the circumstances

sanitary existing at the time of the action, and on the other hand, the erasure

instantaneous data of the terminal by which they were captured, guarantees the

minimization of risks in treatment.

Yes, well, if a less invasive data collection was possible, but this

possibility would be detrimental to the security of the agents and

individuals, by extending the time of interpersonal contact, and in the case of

agents, this increased risk rises exponentially in acts

crowds like the one that caused the identification that is now being evaluated, without

detriment of the fact that against his will and in compliance with his

obligations, can also act as vectors of contagion.

For this reason, the need and suitability of the medium used is considered accredited.

in this specific action in order to reduce contact times

interpersonal relationships, and maintain the social distance that the health authorities

they had been demanding, and that police identification would not violate the principle of

data minimization.

SIXTH.- Finally, and in relation to the qualification of the facts, the

They are included in the serious offense, typified in article 73.f) of the

LOPDGDD, which includes the infraction consisting of: "f) The lack of adoption of

those technical and organizational measures that are appropriate to

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

terms required by article 32.1 of the RGPD".

This conduct would not coincide with the facts prosecuted, insofar as the

identification diligence carried out by the agents was solely

oriented to the prevention of acts typified as a crime in view of

facts with similar antecedents and causes, being on the contrary

police actions covered by the LOPSC and executed based on the

principle of proportionality, suitability and minimum intervention, given that

they only intended to guarantee citizen security and avoid the

consummation of criminal acts through prevention, guaranteeing with the

instant deletion of images the level of security appropriate to the

treatment of the data carried out in the pandemic situation".

SEVENTH: On 02/22/22, the test practice period began,

remembering in the same: a).- to consider reproduced for evidentiary purposes the complaint

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

generated that are part of file E/07313/2020 and b).- consider reproduced

evidentiary effects, the allegations to the initiation agreement of PS/00509/2021,

presented.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

EIGHTH: On 03/10/22, the proposed resolution was transferred to the DGP, in which, it was proposed that, by the Director of the Spanish Agency of Protection of Data a warning was directed to said Body, for the infraction of article 32.1 of the RGPD, when processing the personal data of the claimant, by taking a photograph of his ID with a mobile phone personnel of the police officer, without the required security guarantees for this type of acts.

NINTH: The resolution proposal was notified to the DGP, which, dated 03/17/22, submits a brief of allegations, indicating, among others, the following:

I.- Regarding the identification diligence.

Organic Law 4/2015 of March 30, on security protection citizen (hereinafter, LOPSC), referring, firstly to the preamble where it is indicated that "... the competent authorities are empowered to agree on different actions aimed at maintenance and, where appropriate, at Restoration of citizen tranquility in cases of insecurity public, precisely regulating budgets, purposes and requirements to carry out these procedures, in accordance with the principles, among others, of proportionality, minimal interference and non-discrimination…".

In articles 9 of the same norm, on the obligations and rights of the holder of the National Identity Document and article 16.1, the 3

assumptions in which the Security Forces and Bodies may require the identification of persons ("When there are indications that they have been able to participate in the commission of an offence, when it is necessary to prevent a crime…"), and allusion is made to the strict respect for the principles of proportionality, equal treatment and non-discrimination on the grounds of birth, nationality, racial or ethnic origin, sex, religion or belief, age, disability, sexual orientation or identity, opinion or any other personal or social condition or circumstance, which must necessarily govern the practice of identification diligence.

Needless to say, the police action was carried out with absolute respect for the principles contained in article 16.1 LOPSC (proportionality, equality of treatment and non-discrimination), extremes that the claimant has not questioned, focusing the complaint of this only in the means used for the practice of the identification.

The use of electronic devices is becoming more common in the different police services and its purpose is to expedite police actions, optimizing available resources without undermining guarantees citizens and reducing intervention times, which results in the standards of quality of the police service and in the security of the own acting.

Article 16.2 LOPSC, does contemplate the use of any means available of the agents that favors the act of identification. Article 16.2 LOPSC.- When identification is not possible by any means, including the

telematic or telephone, or if the person refuses to identify himself, the agents,

to prevent the commission of a crime or in order to punish an infraction,

may require those who cannot be identified to accompany them to

the nearest police stations (...).

Based on this authorization, which refers to the use of any means, without limiting

strictly to official or endowment means, the official who carried out this

diligence, he used the means available to him, in this case a

particular mobile device, for not having another device at that time

officer at your disposal, and taking into account the exceptional circumstances of the

international pandemic context caused by the SARS-CoV-2 coronavirus,

in order to practice identification with a medium that facilitated the intervention

minimizing interpersonal contact, as has been said

previously, following the instructions of the health authorities when

respect and with scrupulous respect for data protection regulations

in regard to the treatment of this personal data because, as already

indicated, once the necessary checks were made, the images were

deleted without leaving any trace of them in any file

police or private

4 It can be stated, therefore, that police action for crime prevention and

maintenance of public order specifically accommodated the principles

basic actions established in article 5 of Organic Law 2/1986,

of March 13, Security Forces and Bodies, as well as the

forecasts of the LOPSC itself.

II.- Applicable regulations regarding the protection of personal data.

The act that gives rise to this procedure consists of the diligence of

identification that was made during a concentration in Madrid,

on 06/01/21.

The identification diligence, as extracted from the articles before

referred to the LOPSC, is part of the activity that, in terms of

prevention of criminal and administrative infractions, carried out by the Forces and

Security forces. It should be noted again that many

concentrations or demonstrations, are usually used by individuals or

groups that sheltered in the crowd carry out criminal acts that

must be prevented by the Security Forces and Bodies to guarantee

citizen security and the free development of fundamental rights and

public freedoms of other citizens.

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

Personal and guarantee of digital rights, alleged by the AEPD for

initiate the sanctioning procedure, expressly excludes from its scope of

application to this matter, determining in article 2.2 of the same:

Article 2 LPDGDD.- 2. This organic law shall not apply: a) To the

treatments excluded from the scope of application of the General Regulation of

data protection by its article 2.2, without prejudice to the provisions of the

sections 3 and 4 of this article.

In this sense, article 2.2.d) of Regulation (EU) 2016/679, of the

European Parliament and of the Council, of April 27, 2016, regarding the
protection of natural persons with regard to data processing
personal data and the free circulation of these data, regulates the scope of application
material of the same, and excludes the treatment of personal data carried out by
part of the competent authorities for the purposes of prevention, investigation,
detection or prosecution of criminal offenses, or execution of
criminal sanctions, including protection against security threats
public and its prevention.

For all of the above, the references that in the Resolution Proposal of
Sanctioning Procedure are carried out to this Organic Law 3/2018, of 5 of
December, are incorrect, to the extent that the matter to which it deals
is expressly excluded from its scope of application.

Thus, there is no doubt that, on the date on which the events take place
object of this procedure, the processing of personal data by
of the competent authorities for purposes of prevention, investigation,
detection or prosecution of criminal offenses or execution of
criminal sanctions, at the time of the events that gave rise to this
sanctioning procedure, were already subject to regulation by the Organic Law
7/2021, of May 26, on the protection of personal data processed for purposes
of prevention, detection, investigation and prosecution of infringements
penalties and execution of criminal sanctions, issued in transposition of the
Directive (EU) 2016/680 of the European Parliament and of the Council, of April 27
of 2016, relative to the protection of natural persons with regard to
processing of personal data by the competent authorities to
purposes of prevention, investigation, detection or prosecution of violations
criminal offenses or the execution of criminal sanctions, and the free circulation of said

data.

III.- Regarding the merits of the matter:

Notwithstanding the foregoing, and the clear exclusion of the LPDGDD for exceeding

of the scope of application of the matter dealt with, the Resolution Proposal

performs in the Basis of Law III, an analysis of the alleged

excessive treatment of personal data of protesters: reaching the

following conclusion:

(...) That given the social-health context due to the pandemic that

we were suffering, the high risk of contagion by the Covid-19 virus was assessed.

19, which has been found to multiply in these massive acts,

therefore, he proceeded to take a photograph of the claimant's DNI, the only

objective of avoiding the manipulation of this and maintaining the safety distance

and that, once the necessary checks were made, he deleted it

immediately from the device. To clarify below that, "the fact that

that it be advised to take extreme precautions and expedite as much as possible the

interventions with the demonstrators, using an exceptional means of

identification such as taking pictures with a mobile phone made it possible, in

the work of identifying the protesters reduced contact

interpersonal relationship between them and the agents. All this added to the fact that, once made

the necessary verifications in the identification, the images taken with

the mobile were erased.

Finally, it considers the aforementioned resolution that “the realization of the photograph of the claimant's DNI, in the exceptional circumstances of the pandemic experienced, complies with the principle of minimization of the data, collected in the article 5.1.c) of the RGPD, that is: “adequate, pertinent and limited to the necessity”, for which they were collected.”

In the following Legal Basis, the taking of the DNI photograph is analyzed of the claimant with the private mobile phone of the National Police agent:

In this sense, it considers the fact that the photograph of the DNI of the particular was made with the private mobile phone of the civil servant of policeman.

Regarding this circumstance, from the Deputy Directorate of Operations of the DGP, instructions have already been issued in order to ensure compliance of police actions with the regulations on the Protection of Data, instructions that were disseminated to all police units to your knowledge.

Reference is made in this Legal Basis to article 32 of the RGPD, which requires data controllers to adopt the corresponding security measures of a technical and organizational nature necessary to guarantee that the treatment is in accordance with the regulations in force, as well as to guarantee that any person acting under the authority of the person in charge or the person in charge and has access to personal data only those can treat following instructions of the person in charge.

It then refers to section 1.b) of the aforementioned article 32, which refers to the following: "Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of varying probability and severity to the rights and

freedoms of natural persons, the person in charge and the person in charge of the

treatment will apply appropriate technical and organizational measures to

guarantee a level of security appropriate to the risk, which, where appropriate, includes,

among others: (...) b).- The ability to guarantee confidentiality, integrity,

permanent availability and resilience of treatment systems".

Finally concluding that: "in this case, where the police agent carried out

a photograph of the claimant's ID with his mobile phone for personal use,

does not guarantee a level of security adequate to the required requirements,

circumstance that would not occur if said photograph had been taken with a

official device.

"FIRST.- The Organic Law 7/2021, which has previously been made

reference regarding its preferential application because it is a special law regarding the

general regulations for the protection of personal data processed by the

competent authorities for the purposes of prevention, investigation, detection or

prosecution of criminal offences, as well as the Directive of the Parliament

European and Council, 680/2016, also contain their own regulation

Regarding the security of the treatment, thus article 37 of LO 7/2021 is

determines that: 1. The controller and the processor, taking into account

account the state of the art and the costs of application, and the nature,

scope, context and purposes of the treatment, as well as the levels of risk

for the rights and freedoms of natural persons, will apply measures

appropriate technical and organizational measures to guarantee a level of security adequate, especially with regard to the treatment of the categories of personal data referred to in article 13.

This article does not mention the ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems, which is mentioned in the Agency's resolution and which it does contain the GDPR.

However, it does expressly mention that they must be taken into account different circumstances such as: the context of the treatment, to which so many times has been alluded to in the development of this procedure, the context in which unwrapping the id in question was a completely unwrapped context anomalous, in which the global pandemic situation caused by COVID, demanded that health protection measures be taken for both law enforcement officers police as well as individuals, were interposed to other circumstances in other priority contexts, causing them to relax certain protocols and modes of action in order to give priority to health security.

In this context, it must be clarified that it appeared so unexpectedly and supervening, which did not allow the adoption by the Administrations Public, with sufficient technical means to guarantee that all officials had the appropriate official tools to guarantee that these functions of protection and prevention of citizen security in crowded environments were developed with the means that in terms of data processing would be desirable. Thus, it was left to the discretion of the officials the adoption of the measures that, in their case, they considered opportune to protect your safety and that of individuals, always acting under the principles of legality and responsibility required by art.

6 of the LO 2/1986, of May 13, on Security Forces and Bodies, and with

respect for the rights of individuals regarding the processing of their data

personal.

This article also alludes to the levels of risk for the rights and

freedoms of natural persons. In this sense, we must stop to analyze

the specific circumstances surrounding the police action. On the one hand, the

technical security measures of the device used (the private telephone of

the official), once the Superior Police Headquarters had been consulted on this

extreme, reports that the terminal used had the following measurements

of security:

1.- Encryption of all personal data, protected by "protection" technology

of data" mechanism by which the files and the keychain of this are protected,

password with key, as well as by FACEID, not being able to access the terminal

mobile without them.

2.- The mobile terminal during the entire collection, as well as transfer of the data to

another support was without internet connection.

3.- That likewise there is no connectivity activated between the gallery of

photos and cloud storage applications or any other

third party application.

4.- Reiterate that the collection of this personal data was done without the

photographic image of the holder of the document, being therefore identical data to

those that had been made in written format.

5.- It should also be pointed out that data collection in paper format shows more lack of security than taking it with technological means, as can be be the impossibility of its immediate elimination by having to rely on special containers for its destruction, as well as security in case of loss.

In addition to the above, the following factors must be taken into account:

a) The term of conservation of the personal data of the individual: in view of the report sent by the agent proceeded to delete the image of the document a Once the purpose for which it was taken has been fulfilled, that is, the data was obtained and preserved for a few minutes, the time it took to carry out the effective identification of the individual, after which, were deleted from the device without any trace of storage of the same or in any other file.

b) The constant custody of the data by a police officer National. Since the photograph was not sent to any other device, not leaving the official's private device at any time and therefore within its scope of control, a fact that, together with the rest of the measures of certainty that the device used counted notably ensures the treatment safety.

c) We must also consider that the alternative to this procedure of the official would have been the handwritten copy of the individual's data for a then communicate them through the station and carry out the timely checks. First of all, it means that this option requires a time of interpersonal contact greater than that of taking the photograph (given that it was intended to avoid as much as possible manipulation by

officials of hundreds of identity documents), and therefore greater

risk of contagion.

On the other hand, these handwritten data are also in the custody

of the official, responsible in its case for its loss or misplacement, if

well, with respect to these 9 actions, the responsibility of the

police officers, who are subject to a statute

professional, disciplinary regime and ethical codes, containing strict

basic principles of action; we are talking (among others) about the

principles contained in the L.O. 2/1986, of May 13, on Forces and Corps

Security, specifically, the principle of responsibility (art. 5.6) according to the

which police officers “are personally and directly responsible for

the acts that they carry out in their professional performance, infringing or

violating the legal norms, as well as the regulations that govern their

profession and the principles set forth above, without prejudice to the

patrimonial responsibility that may correspond to the Administrations

Public for the same.”.

In the present case, it can be affirmed in view of the result of the facts

that the official acted at all times under the aforementioned principle of

responsibility, and proof of this, is that the personal data of the individual

were treated with the sole purpose of preventing citizen security

(art. 1 of LO 7/2021), and guaranteeing that the individual did not suffer any

damage derived from said treatment.

SECOND.- Article 83 of the General Data Protection Regulation

establishes the general conditions for the imposition of fines

administrative. In the second section of the same, the following is determined:

When deciding the imposition of an administrative fine and its amount in each case

individual, due account shall be taken of:

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

nature, scope or purpose of the processing operation in question

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

damages they have suffered; the purpose of the treatment is founded on the

compliance with the tasks of prevention of citizen security for the

that Organic Law 4/2015 attributes powers to the FFCCSS, ordering

the use of the available means in order to guarantee the identification of

people in order to ensure the prevention and maintenance of

citizen security, that is, the personal data was not processed to

other purposes than those established in art. 1 of LO 7/2021, of 26

May. The seriousness of the infringement must be estimated as negligible, in view of the

absence of damage to the person who owns the data, the same can be said

regarding the duration of the infraction, once the brevity of the

treatment.

b) intentionality or negligence in the infringement; not appreciated here

any kind of negligence in the actions of the police officer, every time

that the 1 Supplementary application to LO 7/2021, as deduced from the

art.2.3 LOPDGDD when it provides that "the treatments to which it is not

directly applicable Regulation (EU) 2016/679 for affecting activities

not included in the scope of application of European Union law,

shall be governed by the provisions of their specific legislation, if any, and additionally by what is established in the aforementioned regulation and in this law Organic". 10 performance was carried out with all security measures necessary to guarantee the success of the police intervention, the security of personal data, and more importantly, health of officials and individuals.

c) any measure taken by the controller or processor to alleviate the damages suffered by the interested parties; as has already been advance, the individual did not suffer any damage derived from the treatment of his personal data, but a fortiori, the Deputy Directorate of Operations has adopted measures to prevent the use of private electronic devices in order to identify people, which have consisted, on the one hand, in the dissemination to the entire scope of this Directorate, of operating instructions referred to the practice of identifications, and on the other hand, it is found in advanced state of elaboration, of a regulatory provision of a that will regulate the use of mobile recording devices by police officials, in order to adapt the new protocols, to the postulates of the L.O. 7/2021, of May 26.

d) the degree of responsibility of the person in charge or of the person in charge of the treatment, taking into account the technical or organizational measures that have applied under articles 25 and 32;

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

treatment; There is no record of the existence of complaints for facts

similar, this measure being exceptional and derived from the transitory situation

caused by the pandemic situation caused by the COVID SARS virus

19, so it can be stated that there has been no recidivism in these cases.

facts.

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

remedying the violation and mitigating the possible adverse effects of the violation:

In this sense, it must be specified that no activity has been necessary

complementary intended to mitigate the adverse effects since it has not been

produced any damage. All the efforts of the control authority have been

focused on the adoption of preventive measures aimed at regulating the

use of electronic devices and their adaptation to the recent regulation of

Data Protection. g) the categories of personal data

affected by the infringement. As reported by the police officer, the

photograph of the document was limited to personal data relating to: Name,

surnames, sex, nationality, date of birth, issuance of the document and

validity, as well as support number and document number, without it being

photographed the image of the same, therefore, categories have not been treated

special data, whose protection is reinforced by law, despite

of the express authorization for its treatment by the Forces and

Security Corps, provided for in art. 13 of LO 7/2021.

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

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

to what extent; Although it is true that the control authority had

knowledge of the facts that make up the alleged infringement by complaint

of the individual, and not by this Directorate, this is mainly due to the fact that

Based on the legal grounds set forth in this document,

no administrative fault is observed in the practice of identifying the

given the exceptional context in which it was developed.

On the other hand, it should be noted that in addition to admitting the reality of the facts,

all the actions have been directed from its knowledge to reinforce

the prevention of behaviors that could be contrary to the regulations

personal data protection regulator.

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

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

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

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

certificates approved in accordance with article 42, and

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

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

or indirectly, through infringement. In this sense, to argue that the only

advantage resulting from the way in which the police officer acts, can

be derived for citizen safety, as well as for the safety and health of

those involved in the police intervention (officials and individuals), since the

The purpose of this decision was none other than to facilitate the identification of this

person, in a crowded context, avoiding contact as much as possible, and

speeding up the intervention for the sake of safety, without forgetting in any

moment the security of the processing of personal data.

THIRD.- This article was duly transposed into Spanish regulations,

being reflected in article 76 of the L.O. 3/2018, of December 5, of

Protection of Personal Data and guarantee of digital rights, which

establishes that: 2. In accordance with the provisions of article 83.2.k) of the RGPD

to take into account: a) The continuous nature of the infraction. not appreciated

such character in the intervention object of the present procedure. b) The

linking the activity of the offender with the performance of treatment of

personal information. The processing of personal data becomes a competence

directly from the General Directorate of the Police, by virtue of the powers

assigned to this police force by the L.O. 2/1986, of May 13, Forces

and Security Bodies, as well as by the L.O. 4/2015, of March 30, of

protection of citizen security. c) The benefits obtained as

consequence of the commission of the offence. Needless to say, it has not been

obtained greater benefit with the intervention carried out beyond the derivative

for public safety and the health of those involved. d) The possibility of

that the conduct of the affected party could have induced the commission of the

infringement. e) The existence of a merger process by absorption subsequent to the

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

The rights of minors have not been affected. g) Arrange, when not

mandatory, of a data protection delegate. h) Submission by

part of the person in charge or in charge, on a voluntary basis, to mechanisms of

alternative conflict resolution, in those cases in which there are

controversies between them and any interested party.

Based on all the above, and taking into account all these circumstances

analyzed, which article 83 urges to consider when deciding on

the imposition of an administrative sanction, it can be concluded that the action

of the police was adjusted to contextual needs.

Therefore, having accredited the need and suitability of the medium used for the

effects of reducing interpersonal contact times, and maintaining the

social distance that the health authorities imposed in order to prevent

successive infections, and in view of the security measures adopted in the

development of the analyzed intervention, this Directorate General understands that the

identification of the individual, was covered with security guarantees

required, not proceeding therefore, the imposition of the sanction of

warning proposed by the examining body, for which reason it is urged to file

of this proceeding without imposition of any sanction".

Of the actions carried out in this procedure, of the information and

documentation presented by the parties, the following have been accredited:

PROVEN FACTS

First: The claimant, when he tried to leave the demonstration in which he was

participating, a police control that was in one of the streets adjacent to

the demonstration required them to identify themselves. When he showed them his ID, one of the

agents took a photograph of the document and returned it to him.

Second: Given these facts, the DGP stated to this Agency, among others, that the

data processing carried out by the police officer when taking the photograph of the DNI

of the claimant with the camera of his private mobile phone was a way of proceeding

exceptional in the circumstances of the pandemic experienced, in order to avoid a risk to

your health.

Third: The DGP affirms before this Agency that, from the Deputy Directorate of Operations,

Instructions will be given on the use of electronic devices by

part of police officers in operational actions, in a way that ensures

the conformity of said actions to the regulations on the Protection of

Data.

FOUNDATIONS OF LAW

I.- Competition:

The Director of the Spanish Agency is competent to resolve this procedure.

Data Protection, in accordance with the provisions of art. 58.2 of the RGPD in

the art. 47 of LOPDGDD.

II.- Summary of the facts:

According to the claimant, when he tried to leave the concentration in which they were

participating, a police control that was in one of the streets adjacent to

the concentration required him to identify himself. When he showed them his ID, one of them

he took a picture of the document with his personal mobile phone and handed it back. The

The claimant assures that the agent herself told her that the photographs were

taking with his personal mobile phone, since they did not have an official telephone number.

On the part of the DGP, it was stated that, in the social and health context such as the one

was living, marked by the coronavirus COVID-19, the practice of identifying
people implied an increase in personal risk to the health of the
agents so in cases like this, self-protection measures were extreme
avoiding all direct contact with the people who identified themselves and with their
belongings, looking for environmental conditions of asepsis and keeping distances
of security, reason why it was decided that the best solution for it, was the taking of
photographs of the DNI, ensuring that, once the appropriate checks have been made
for correct identification, the photograph was immediately deleted from the device.

III.- Regarding the allegations made by the DGP regarding the proposal for
resolution.

FIRST: The DGP alleges in its brief dated 03/17/22 that article 2.2.d) of the
RGPD, excludes from its application the processing of personal data carried out by
of the competent authorities for the purposes of prevention, investigation, detection or
prosecution of criminal offences, or execution of criminal sanctions, including
that of protection against threats to public security and their prevention, and that,
Therefore, the data processing carried out by the police officer when taking the photograph
of the claimant's DNI with the camera of the private mobile phone is
expressly excluded from the scope of application of the RGPD and the LOPDGDD.

In this regard, the following should be indicated:

Organic Law 4/2015, of March 30, on the Protection of Citizen Security
(LOPSC), empowers the competent authorities to:

“(…) agree on different actions aimed at maintenance and, where appropriate, at
Restoration of citizen tranquility in cases of insecurity
public, precisely regulating budgets, purposes and requirements
to carry out these procedures, in accordance with the principles, among others, of
proportionality, minimal interference and non-discrimination (…)”.

In application of the foregoing, article 9.2 of the LOPSC establishes, with respect to the

obligation to show the DNI to the agents of the Security Forces and Bodies of the

State, the following:

"two. All persons required to obtain the National Document of

Identity they are also to exhibit it and allow the verification of the

security measures referred to in section 2 of article 8 when

are required to do so by the authority or its agents, for the

compliance with the purposes set forth in section 1 of article 16.

theft or loss must be reported as soon as possible to the

Police station or post of the Security Forces and Corps more

next".

For its part, article 16 of the LOPSC itself, on the possibility of verifying

of the DNI by the State Security Forces and Bodies, establishes that:

1. In the fulfillment of its functions of criminal investigation and prevention,

as well as for the sanction of penal and administrative infractions, the agents

of the Security Forces and Bodies may require the identification of the

people in the following cases:

a) When there are indications that they may have participated in the commission of a

infringement.

b) When, in view of the concurrent circumstances, it is considered

reasonably necessary to prove their identity to prevent the commission

of a crime. In these cases, the agents may carry out the

necessary checks on public roads or in the place where the

made the request, including the identification of persons whose face was not

is totally or partially visible due to the use of any type of garment or object

that covers it, preventing or hindering identification, when necessary to

the indicated effects (…)".

However, in the LOPSC Law itself, certain limits are established to this practice of

verification of the DNI, indicating that:

"(…) In the practice of identification, the

principles of proportionality, equal treatment and non-discrimination on grounds

of birth, nationality, racial or ethnic origin, sex, religion or belief,

age, disability, sexual orientation or identity, opinion or any other

personal or social condition or circumstance (…)".

The National Security Scheme, regulated in Royal Decree 3/2010, of 8

January, modified by Royal Decree 951/2015, of October 23, establishes, in its

article 21, the following:

"In the structure and organization of the security of the system, it will be paid

particular attention to information stored or in transit through

insecure environments.

Portable equipment will be considered insecure environments,

personal assistants (PDA), peripheral devices, information carriers and

communications over open networks or with weak encryption.

2.- Part of security is the procedures that ensure the

retrieval and long-term preservation of electronic documents

produced by public administrations within the scope of their

competencies.

3. All information in non-electronic support, which has been caused or
direct consequence of the electronic information referred to in the
present royal decree, must be protected with the same degree of security
than this one. To this end, the measures that correspond to the nature of the
of the support in which they are found, in accordance with the rules of
application to their safety.

And for its part, article 22 of RD 3/2010, on prevention before other systems
of interconnected information, establishes the following:

“The system has to protect the perimeter, in particular, if it connects to networks
public. Public communications network shall be understood as the network of
electronic communications that is used, in whole or mainly,
for the provision of electronic communications services available
for the public, in accordance with the definition established in section 26
of annex II, of Law 32/2003, of November 3, General of
Telecommunications. In any case, the risks derived from the
interconnection of the system, through networks, with other systems, and
will control your junction point.

Regarding the Activity Register, article 23 of RD 3/2010 establishes that:

“With the exclusive purpose of achieving the fulfillment of the object of this
royal decree, with full guarantees of the right to honor, to personal privacy
and family and in the image of those affected, and in accordance with the regulations

on the protection of personal data, of public or labor function, and other

provisions that result from application, the activities of the

users, retaining the information necessary to monitor, analyze,

investigate and document improper or unauthorized activities, allowing

identify at each moment the person who acts".

And regarding the minimum requirements, article 27 of RG 3/2010 establishes:

1. To comply with the minimum requirements established in this

royal decree, the Public Administrations will apply the security measures

indicated in Annex II, taking into account: a) The assets that constitute the

system. b) The category of the system, as provided in article 43. c) The

decisions taken to manage identified risks.

2. When a system affected by this Royal Decree handles data from

of a personal nature, the provisions of the Organic Law will apply

15/1999, of December 13, and development regulations, without prejudice to the

requirements established in the National Security Scheme.

Note: Rule repealed, with effect from 07/12/18, without prejudice to the

provided for in additional provision 14 of Organic Law 3/2018, of 5

of December, as established in its sole repeal provision) therefore

that this section is understood as referenced to the RGPD and the LOPDGDD,

currently in force)

3. The measures referred to in sections 1 and 2 will have the condition

of minimum requirements, and may be extended due to the concurrence
indicated or the prudent discretion of the person responsible for the information, given
account of the state of technology, the nature of the services provided and the
information handled, and the risks to which they are exposed.

Finally, regarding the security audits of the information systems used,
Article 34 of RD 3/2010 establishes the following:

1. The information systems referred to in this royal decree
shall be subject to an ordinary regular audit, at least every two years, which
verify compliance with the requirements of this National Scheme
of security. On an extraordinary basis, said audit must be carried out
Whenever there are substantial changes in the system of
information, which may affect the required security measures. The
performance of the extraordinary audit will determine the date of computation for
the calculation of the two years, established for the realization of the following
ordinary regular audit, indicated in the previous paragraph.

2. This audit will be carried out based on the category of the system,
determined according to the provisions of annex I and in accordance with the provisions of
annex III.

3. Within the framework of the provisions of article 39, of Law 11/2007, of 22
June, the audit will delve into the details of the system to the level that
considers that it provides sufficient and relevant evidence, within the scope
established for the audit.

4. In carrying out this audit, the criteria, methods of
generally recognized work and conduct, as well as the normalization
national and international applicable to this type of audits of systems of
information.

5. The audit report must rule on the degree of compliance with the

present royal decree, identify its deficiencies and suggest possible measures

necessary corrective or complementary, as well as the recommendations that

are considered appropriate. It must also include the criteria

audit methodologies used, the scope and objective of the audit, and

the data, facts and observations on which the conclusions are based

formulated.

6. The audit reports will be presented to the person in charge of the system and to the

competent security officer. These reports will be analyzed by

the latter who will present his conclusions to the person in charge of the system for

take appropriate corrective action.

Therefore, taking into account the risks indicated, it should be considered that the use of

personal cameras or cell phones, unofficial or endowed, of the agents does not guarantee

the security of the data, while the private uses that each person can

perform with their own devices are not compatible with the measures of

security that for the exercise of police functions must be adopted by the

responsible for the police file of which such recordings will be part.

SECOND: Regarding the statement made by the DGP when it indicates that: “(…) In this

In this way, it was left to the discretion of the officials to adopt the measures that, in their case,

considered appropriate to protect their safety and that of individuals, always

acting under the principles of legality and responsibility required by art. 6 of the

IT. 2/1986, of May 13, on Security Forces and Bodies, and with respect to the

rights of individuals regarding the processing of their personal data (...)".

It should be noted in this regard that the first additional provision of the LOPDGDD,

on "Security measures in the public sector" establishes that:

1. The National Security Framework will include the measures that must

be implemented in case of processing of personal data to prevent its loss,

alteration or unauthorized access, adapting the criteria for determining the

risk in the treatment of the data as established in article 32 of the

Regulation (EU) 2016/679.

2. Those responsible listed in article 77.1 of this organic law

They must apply to the processing of personal data the measures of

security that correspond to those provided for in the National Scheme of

Security, as well as promoting a degree of implementation of measures

equivalents in companies or foundations linked to them subject to

to private law.

In cases where a third party provides a service under a concession regime,

management assignment or contract, the security measures are

will correspond to those of the original public Administration and will adjust to the

National Security Scheme.

The DGP, as a Body of the Ministry of the Interior, is subject to the provisions of

section 2 of the aforementioned additional provision and since it is the DGP that acts as

responsible for the processing of personal data, it is your obligation to apply to the

processing of personal data carried out by its officials, the measures of

corresponding security, of those provided for in the National Security Scheme,

not being protected by the regulations, leave "(...) at the discretion of the officials the

adoption of the measures that they considered appropriate to protect their

security and that of individuals (...)",

THIRD: About the statement made by the DGP when it indicates that. "(…) It can

affirm in view of the results of the facts that the official acted in all

moment under the aforementioned principle of responsibility, and proof of this, is that the data

personal data of the individual were treated with the sole purpose of preventing the

citizen security (art. 1 of LO 7/2021), and guaranteeing that the individual does not

suffered any damage derived from said treatment (…)".

Indicate in this regard that, as established in its twelfth final provision, this Law

Organic "will enter into force twenty days after its publication in the Official Gazette of the

Condition. Its publication occurred on 05/27/21, so the entry into force of the

standard occurred on 06/16/21.

Well, since the events that are the subject of this proceeding occurred on

06/01/21, the date on which Organic Law 07/2021 was not yet in force, is not

can be taken into account in this case.

FOURTH: Regarding the consideration requested by the DGP, in the sense of applying the

extenuating circumstances indicated in article 83 of the RGPD and in article 76 of the LOPDGDD.

Regarding this aspect, it should be noted that article 77.2 of the LOPDGDD establishes the

Next:

“When those responsible or in charge listed in section 1

committed any of the offenses referred to in articles 72 to

74 of this organic law, the data protection authority that results

authority will issue a resolution sanctioning them with a warning

(…)",

Therefore, it is not possible, in this case, to take into consideration what is stipulated in the

article 83 of the RGPD and in article 76 of the LOPDGDD, in order to graduate the

sanction to be imposed, because in this case, it is only possible to sanction with a warning.

IV.- On the infringement of article 32 of the RGPD committed by the DGP.

The RGPD, in its article 32, requires those responsible for the treatment to adopt,

security measures of a technical and organizational nature that guarantee that the

processing of personal data is carried out in accordance with current regulations, as well

as that, any person acting under the authority of the person in charge or the

person in charge performs it following the instructions of the person in charge and this is established in

said article:

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

natural persons, the person in charge and the person in charge of the treatment will apply

appropriate technical and organizational measures to ensure a level of

security appropriate to the risk, which, where appropriate, includes, among others:

a) pseudonymization and encryption of personal data;

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

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration shall be given to taking into account the risks presented by the processing of data, in particular as consequence of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the unauthorized communication or access to said data.

3. Adherence to an approved code of conduct under article 40 or to a certification mechanism approved under article 42 may serve as a element to demonstrate compliance with the requirements established in the paragraph 1 of this article.

4. The person in charge and the person in charge of the treatment will take measures to ensure that any person acting under the authority of the controller or of the person in charge and has access to personal data can only treat said data following the instructions of the person in charge, unless it is obliged to do so under the law of the Union or of the Member States.

V.- Typification and Sanction for the infringement of article 32.1 of the RGPD

In the present case, the fact of taking a photograph of the DNI with a mobile phone of personal use of a police officer supposes the commission of the infraction of the article 32.1 of the RGPD, when processing personal data without having the guarantees necessary to have implemented the technical and organizational measures appropriate to guarantee a level of security appropriate to the risk.

In this sense, article 73.f) of the LOPDGDD, considers "serious", for the purposes of

prescription, “f) The lack of adoption of those technical and organizational measures that

are appropriate to guarantee a level of security appropriate to the risk of the

treatment, in the terms required by article 32.1 of the RGPD”.

This infraction can be sanctioned with a fine of €10,000,000 maximum 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

of greater amount, in accordance with article 83.4.a) of the RGPD.

In the present case, since the party claimed is the General Directorate of the Police,

Directive Body belonging to the General Administration of the State, it must have

present what is established in art. 83.7 of the aforementioned RGPD, where it is indicated that:

"Without prejudice to the corrective powers of the control authorities (...) each

Member State may lay down rules on whether, and to what extent,

impose administrative fines on authorities and public bodies established in

that Member State".

Well, article 77.2 of the LOPDGDD establishes, on the regime applicable to

Entities that are part of the Public Administration, the following:

“When those responsible or in charge listed in section 1 committed

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

organic, the data protection authorities that are competent will dictate

resolution sanctioning them with a warning. The resolution will establish

Likewise, the measures that should be adopted to stop the conduct or correct it.

the effects of the infraction that has been committed".

In accordance with these criteria, it is considered appropriate to sanction with a warning the General Directorate of the Police, for the infringement of article 32.1 of the RGPD, by considers that the taking of the photograph of the claimant's DNI with a telephone personal mobile of one of the police officers, is an act that does not guarantee a level security appropriate to the risk.

Therefore, in accordance with the foregoing, by the Director of the Agency Spanish Data Protection,

RESOLVES:

FIRST: SANCTION with a WARNING, to the GENERAL DIRECTORATE OF THE POLICE for the violation of article 32.1) of the RGPD, punishable in accordance with the provided in art. 83 of the aforementioned rule, regarding the lack of security in the treatment of personal data revealed at the time of taking a Photograph of the claimant's ID with a personal mobile phone of the police officer who made the identification.

SECOND: NOTIFY this resolution to the GENERAL DIRECTORATE OF THE POLICE and the claimant about the result of the claim.

THIRD: COMMUNICATE this resolution to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

In accordance with the provisions of article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure as prescribed by the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure Common to Public Administrations, and in accordance with the provisions of the art. 112 and 123 of the aforementioned Law 39/2015, of October 1, interested parties may file, optionally, an appeal for reconsideration before the Director of the Agency

Spanish Data Protection Authority within a month from the day

following the notification of this resolution or directly contentious appeal

before the Contentious-Administrative Chamber of the National High Court,

in accordance with the provisions of article 25 and paragraph 5 of the provision

additional fourth of Law 29/1998, of July 13, regulating the Jurisdiction

Contentious-Administrative, within two months from the day after

to the notification of this act, as provided in article 46.1 of the aforementioned Law.

Sea Spain Martí.

Director of the Spanish Agency for Data Protection.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es