 Procedure No.: PS/00523/2021

RESOLUTION OF THE PUNISHMENT PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency before

the COMMUNITY OF PROPRIETORS R.R.R., with CIF.: ***NIF.1 (hereinafter, “the part

claimed"), by virtue of a complaint filed by A.A.A., (hereinafter, "the party

claimant"), for the alleged violation of data protection regulations:

Regulation (EU) 2016/679, of the European Parliament and of the Council, of 04/27/16,

regarding the Protection of Natural Persons with regard to the Treatment of

Personal Data and the Free Circulation of these Data (RGPD); the Organic Law

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

Digital Rights (LOPDGDD), and attending to the following:

BACKGROUND:

FIRST: On 08/27/20, this Agency received the document submitted

by the claimant, in which, in essence, it was claimed that, to access the swimming pool

of her community, required her to identify herself as the owner by presenting

of your DNI and your personal data that were registered by the security guard of

the installation, on a blank sheet of paper in view of all, there being no document

next to the guard in which he indicated what was going to be done with that data.

The following documentation is attached to the written claim:

a).- Copy of circular dated 07/03/20 where it is stated that the Board of Directors agreed

the opening of the pool with conditions such as the one controlled by the security guard

compliance with sanitary and capacity measures. There is no need to

Identify yourself with your ID.

b).- Copy of police report No. 10113/20, which was drawn up when the claimant called

to the police by not letting her enter the community pool if she did not show her ID.

c).- Photograph of information poster existing in the community of neighbors, dated

07/24/20, where the following information was stated: “it is necessary that you show your

national identity document to the pool controller since the registration of

daily access to such premises may be required at any time by the authority

authority for reasons of public health.

SECOND: Dated 10/07/20, by this Agency and in relation to the

stipulated in article 65.4 of the LOPDGDD Law, a written document was sent to the

claimed requesting information on the aspects outlined in the claim.

According to a certificate from the State Post and Telegraph Society, the requirement

sent to the claimed party, on 10/07/20, through the notification service

Correos postcards was delivered at destination on 10/23/20, identifying the

receiver with ID number: ***NIF.2

THIRD: On 01/08/21 by the Director of the Spanish Agency for

Data Protection agreement is issued for the admission of processing of the claim

presented, in accordance with article 65 of the LPDGDD Law, when assessing possible

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

of the Spanish Agency for Data Protection.

FOURTH: On 07/08/21 and 09/21/21, by the General Subdirectorate of

Data Inspection addressed two separate writings of information request to the part

claimed, under the investigative powers granted to the authorities of

control in article 57.1 of the RGPD, without any response to date.

received in this Agency with respect to said requirements.

FIFTH: On 11/10/21, in view of the facts exposed, the Director of the

Spanish Agency for Data Protection, agreed to initiate a sanctioning procedure against

the party claimed for infringement of article 5.1.c) of the RGPD, when accessing a

excessive amount of personal data of the claimant with respect to the purposes for which

that were intended, imposing an initial penalty of 3,000 euros and for the

Violation of article 13 of the RGPD, by not conveniently informing users of

the community pool of the treatment that was going to be made of your personal data,

when they accessed the community pool, with an initial fine of 3,000 euros.

SIXTH: The initiation of the file was notified on 01/10/22 to the Community of

Neighbors, to date, there is no record that the respondent has made

allegations to the agreement to initiate the procedure.

In this sense, article 64.2.f) of the LPACAP -provision reported by the

claimed in the agreement to open the procedure- establishes that, "if no

they make allegations within the stipulated period on the content of the initiation agreement,

when it contains a precise statement about the responsibility

imputed, may be considered a resolution proposal."

In the present case, the agreement to initiate the disciplinary proceedings determined the

facts in which the imputation was specified, the infraction of the current regulations

attributed to the defendant and the sanction that could be imposed. Therefore, taking into

consideration that the respondent has not made allegations to the agreement to start the

file and in accordance with the provisions of article 64.2.f) LPACAP, the aforementioned

Initiation agreement is considered in this case resolution proposal.

PROVEN FACTS

1º.- The claimant indicates in her writing that, being the owner of the dwelling located in

*** ADDRESS.1 for 15 years, when trying to use the community pool,

the security guard hired by the community of neighbors asked him to

show the DNI to access the pool, which she refused to be the owner and

be correctly identified. Thus, the claimant asked the security guard

security that informs you of the purpose of collecting personal data and that

show the writing where that rule was.

2º.- The claimant continues to indicate that, after contacting the president of the

community, he told her that it was mandatory to enter the premises to present the

DNI and that there was a law of the Ministry of Health that was well above the

Data Protection Law, since there was the possibility of an outbreak

of "COVID", and the Ministry forced him to ask for the DNI to be able to later get in touch.

contact with neighbors and inform them that they had been in contact, so if

she did not show her ID prohibited her from accessing the community pool.

3º.- Put in contact with the administrator of the farm, he told him that this measure

by "COVID19", was taken exclusively by decision of the Board of Directors of the

community of neighbors, never by the Neighborhood Council, as it was obligatory to do.

to have happened

4º.- A few days later he tried to access the community pool again, but he did not

They allowed her access by refusing to show her ID, so she required the presence

of the police, which drew up a report of the events with number: Nº 45668/2020.

5º.- In addition, the claimant indicates that, when the owners accessed the pool and

presented their DNI to the security guard, he noted the person's data

that he accessed on a blank sheet of paper in view of all and that there was no

document together with the security guard in which he informed of the management that was going to be carried out

with those data.

6º.- On behalf of this Agency, up to three letters have been sent to the Community of

Owners requesting information on the facts indicated by the claimant without

that no response has been received from this Agency in any of them. Either

no brief of allegations has been received at the initiation of the procedure

sanctioning

FOUNDATIONS OF LAW

I.- Competition

Is competent to resolve this Sanctioning Procedure, the Director of the

Spanish Agency for Data Protection, by virtue of the powers that article 58.2 of the

GDPR and arts. 47, 64.2 and 68.1 of the LOPDGDD Law.

II.- On the processing of personal data resulting from the situation arising from the

COVID-19 Virus Spread,

Given the public health emergency situation resulting from the extension of the

COVID19, the Spanish Agency for Data Protection prepared several documents in

related to it to respond to the doubts that arose with the situation that was

lived in the year 2020. Thus, the report of the Legal Office of the AEPD, with N/REF:

0017/2020 indicated, in this regard, the following:

“In the first place, in general, it should be clarified that the protection regulations

of personal data, while, aimed at safeguarding a fundamental right, it is

applies in its entirety to the current situation, since there is no reason

determine the suspension of fundamental rights, nor has said measure been

adopted.

Notwithstanding the foregoing, the GDPR itself contains the safeguards and rules

necessary to legitimately allow the processing of personal data in

situations, such as the epidemic, in which there is a health emergency of

general. Therefore, when applying said precepts provided for these cases in the

GDPR, in accordance with the applicable sectoral regulations in the field of health

public information, considerations related to data protection -within the

limits provided by law - should not be used to hinder or limit the

effectiveness of the measures adopted by the authorities, especially health,

in the fight against the epidemic, since data protection regulations

contains a regulation for such cases that reconciles and weighs the

interests and rights at stake for the common good.

Recital (46) of the RGPD already recognizes that, in exceptional situations, such as

an epidemic, the legal basis for treatments can be multiple, based both on

the public interest, such as in the vital interest of the interested party or another natural person. (46) The

processing of personal data should also be considered lawful when it is

necessary to protect an interest essential to the life of the data subject or that of another

Physical person. In principle, personal data should only be processed on the basis of the

basis of the vital interest of another natural person when the treatment cannot be based

manifestly on a different legal basis.

Certain types of processing may serve both important reasons of interest

public as to the vital interests of the interested party, such as when the

treatment is necessary for humanitarian purposes, including the control of epidemics and their

spread, or in situations of humanitarian emergency, especially in case of
natural or man-made disasters.
Therefore, as a legal basis for lawful processing of personal data, without
Despite the fact that there may be other bases, such as the fulfillment of a
legal obligation, art. 6.1.c) RGPD, the Regulation explicitly recognizes the two
cited: mission carried out in the public interest (art. 6.1.e) or vital interests of the
interested party or other natural persons, (art. 6.1.d).
The art. 6.1, letter d) RGPD considers not only that the vital interest is a sufficient basis
legal nature of the processing to protect the “data subject” (insofar as this is a term
defined in art. 4.1) RGPD as an identified or identifiable natural person), but
said legal basis can be used to protect the vital interests “of another
natural person”, which by extension means that said natural persons can be
even unidentified or identifiable; that is, said legal basis for the treatment (the
vital interest) may be sufficient for the processing of personal data aimed at
protect all those people susceptible to being infected in the spread
of an epidemic, which would justify, from the point of view of data processing
personal information, in the widest possible way, the measures adopted for this purpose,
even if they are aimed at protecting unnamed people or in principle not
identified or identifiable, since the vital interests of said persons
must be safeguarded, and this is recognized by the regulations of
personal data protection.
Section 3 of article 6 GDPR does not establish the need for the basis of the
treatment for reasons of vital interest must be established by the Law of the
Union or the Law of the Member States applicable to the person responsible for the
treatment, since this section refers exclusively to the treatments
established for the fulfillment of a legal obligation, or for the fulfillment of

a mission carried out in the public interest or in the exercise of public powers, both referred to in letters c) and e) of said article 6 RGPD, but not for the treatments included in letter d). c. However, for the treatment of health data it is not enough with the existence of a legal basis of art. 6 GDPR, but in accordance with art. 9.1 and 9.2 RGPD there is a circumstance that lifts the prohibition of treatment of said special category of data (including health data).

(...) In a health emergency situation such as the one referred to in the request for this report, it is necessary to bear in mind that, in the exclusive scope of the of protection of personal data, the application of the regulation of protection of personal data would allow the data controller to adopt those decisions that are necessary to safeguard the vital interests of natural persons, the compliance with legal obligations or the safeguarding of essential interests in the field of public health, within the provisions of the applicable material regulations.

What these decisions are, (from the point of view of the protection regulations of personal data, it is reiterated) will be those that those responsible for the data processing must adopt according to the situation in which they find themselves, always aimed at safeguarding the essential interests already so reiterated. But the data controllers, as they are acting to safeguard said interests, must act in accordance with what the authorities established in the regulations of the corresponding Member State, in this case Spain, establish.

Thus, the Spanish legislator has provided itself with the necessary and timely legal measures

to deal with situations of health risk, such as Organic Law 3/1986, of
April 14, of Special Measures in the Matter of Public Health (modified by
Royal Decree-Law 6/2020, of March 10, which adopts certain
urgent measures in the economic field and for the protection of public health,
published in the Official State Gazette of March 11, 2020) or Law 33/2011,
of October 4, General of Public Health.

Article 3 of the first of these regulations states that: [i]n order to control the
communicable diseases, the health authority, in addition to carrying out the actions
general preventive measures, may adopt the appropriate measures to control the
sick, people who are or have been in contact with them and
of the immediate environment, as well as those considered necessary in case of
transmissible risk. Similarly, articles 5 and 84 of the Law
33/2011, of October 4, General of Public Health refer to the previous Law
organic 3/1986, and the possibility of adopting additional measures in case of risk
of disease transmission.

Therefore, in terms of risk of disease transmission, epidemic, crisis
etc., the applicable regulations have granted "the health authorities of the
different Public Administrations" (art. 1 Organic Law 3/1986, of April 14) the
powers to adopt the necessary measures provided for in said laws when
so required by health reasons of urgency or necessity. Consequently, from a
point of view of processing personal data, the safeguarding of interests
essential in the field of public health corresponds to the different authorities
health authorities of the different public administrations, who may adopt the

measures necessary to safeguard such essential public interests in

public health emergency situations.

These competent health authorities of the different administrations will be

public authorities who must adopt the necessary decisions, and the different

responsible for the processing of personal data must follow these

instructions, even when this involves the processing of personal data of

health of natural persons. The foregoing refers expressly to the possibility

to treat the personal health data of certain natural persons for the

responsible for processing personal data, when, by indication of the

competent health authorities, it is necessary to communicate to other people with whom

that said natural person has been in contact with the circumstance of contagion,

to safeguard both these natural persons from the possibility of contagion

(vital interests of the same) as to prevent said natural persons, for

ignorance of their contact with an infected person can spread the disease to

other third parties (vital interests of third parties and essential and/or qualified public interest

in the field of public health).

However, the processing of personal data in these emergency situations

health, as mentioned at the beginning of this report, continue to be treated

in accordance with the personal data protection regulations (RGPD and Law

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

digital rights, LOPDGDD), so all its principles apply,

contained in article 5 RGPD, and among them that of data processing

personal with legality, loyalty and transparency, of limitation of the purpose (in this

case, safeguard the vital/essential interests of natural persons), principle

accuracy, and of course, and special emphasis must be placed on it, the principle of

data minimization.

Regarding this last aspect, express reference must be made to the fact that the data processed

shall be exclusively those limited to those necessary for the purpose

intended, without this treatment being able to be extended to any other data

personal data not strictly necessary for said purpose, without being able to

confuse convenience with necessity, because the fundamental right to

data protection continues to be applied normally, notwithstanding that, as

has said, the personal data protection regulations themselves establish that in

emergency situations, for the protection of essential health interests

public and/or vital data of natural persons, the health data may be processed

necessary to prevent the spread of the disease that has caused the

health emergency.

Regarding the principle of limitation of the purpose in relation to cases of

processing of health data for reasons of public interest, Recital (54)

RGPD is clear, when it establishes that: The treatment of special categories of

personal data, without the consent of the interested party, it may be necessary for

reasons of public interest in the field of public health. That treatment must be

subject to appropriate and specific measures in order to protect the rights and freedoms

of natural persons. […] This processing of data related to health for reasons

of public interest must not give rise to third parties, such as entrepreneurs,

insurance or banking entities, treat personal data for other purposes.

III.- Regarding the excessive collection of personal data to be able to access the pool of the community of neighbors:

In the present case, the claimant states that, after refusing to present the DNI to access the swimming pool of his community because he considered that it was excessive present the DNI to the security guard, because being the owner, with a seniority of more than 15 years, was sufficiently identified. who contacted the president of the community to denounce the case to which he told him that it was mandatory, to access the premises, present the DNI and that there was a law of the Ministry of Health that was well above the Data Protection Law, since, if If there is an outbreak of covid19, the Ministry forces you to request the DNI to be able to later locate neighbors in case of contagion.

Regarding the excessive use of personal data, recital 39 of the RGPD establishes that: "(…) All personal data processing must be adequate, pertinent and limited to what is necessary for the purposes for which they are treated. This requires, in particular, ensuring that their use is limited to a strict minimum. conservation period. Personal data should only be processed if the purpose of the processing treatment could not reasonably be achieved by other means. To ensure that personal data is not kept longer than necessary, the person responsible for the treatment must establish deadlines for its suppression or periodic review. must take all reasonable steps to ensure that they are rectified or deleted personal data that is inaccurate. Personal data must be treated in a way that guarantees adequate security and confidentiality of the data including to prevent unauthorized access or use of such data and of the equipment used in the treatment.

For its part, article 5.1.c) of the RGPD establishes the Principles related to the

treatment, indicating in this regard that: “Personal data will be adequate,

relevant and limited to what is necessary in relation to the purposes for which they are

processed (“data minimization”);

Well, although in the pandemic situation that was experienced in 2020, the

competent health authorities adopted the necessary measures to stop the

pandemic, and therefore, the different data controllers

personnel had to follow these instructions, even when it meant a

processing of personal health data, if necessary

communicate to other people a possible outbreak in their environment with the aim of

safeguard the health of all, the fact of requesting the personal data included in the

DNI of the claimant, is excessive for the purposes for which they were intended,

because being the owner of a home in the community with an age of more than

15 years old, was sufficiently identified even, only with the indication

of the portal, floor and letter, for example.

Therefore, the exposed facts are clearly constitutive of an infraction,

attributable to the claimed party, for violation of article 5.1.c) of the RGPD, by

request the claimant more personal data than is strictly necessary for the

end that was pursued.

In this sense, article 72.1.a) of the LOPDGDD typifies, for prescription purposes,

as "very serious", the: "treatment of personal data violating the principles and

guarantees established in article 5 of the RGPD”.

This infraction may be sanctioned according to the provisions of article 83.5.b) of the

RGPD, where it is established that: “Infringements of the following provisions are

shall be sanctioned, in accordance with section 2, with administrative fines of 20,000,000

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

as a maximum of the overall annual total turnover of the financial year

above, opting for the highest amount: a) the rights of the interested parties to

tenor of articles 12 to 22”.

In accordance with the precepts indicated for the purposes of setting the amount of the penalty

impose, it is considered appropriate to graduate the sanction in accordance with the following

Aggravating criterion established in article 83.2 of the RGPD:

a).- The duration of the infraction, since it is verified, according to the claimant and the

police that the community of neighbors requested the personal data of all those

who, during the summer of 2020, made use of the facilities of the

swimming pool of the community of neighbors (section a).

The balance of the circumstances contemplated in article 83.2 of the RGPD, with

Regarding the infraction committed by violating the provisions of article 5.1.c) of the

RGPD, allows you to set a penalty of 3,000 euros, (three thousand euros).

IV.- Regarding the lack of information provided to the users of the swimming pool when

asked for the DNI to access the community pool:

According to the claimant, when the owners accessed the community pool and

presented their ID, the security guard noted the personal data of the

person who accessed a blank sheet of paper in view of all, there being no

document together with the security guard that informs about the treatment of the data

personal. Nor were users of the facility informed about the management

which would subsequently be carried out with the personal data obtained from the DNI.

Regarding the information that the person responsible for the processing of personal data

must be provided to the interested parties when they obtain their personal data, the

Article 13 of the RGPD, establishes the following:

"1. When personal data relating to him is obtained from an interested party, the

responsible for the treatment, at the time these are obtained, will provide you with:

a) the identity and contact details of the person in charge and, where appropriate, of their

representative;

b) the contact details of the data protection delegate, if any;

c) the purposes of the treatment to which the personal data is destined and the legal basis

of the treatment;

d) when the treatment is based on article 6, paragraph 1, letter f), the interests

legitimate of the person in charge or of a third party;

e) the recipients or the categories of recipients of the personal data, in their

case;

f) where appropriate, the intention of the controller to transfer personal data to a third party

country or international organization and the existence or absence of a decision to

adequacy of the Commission, or, in the case of transfers indicated in the

Articles 46 or 47 or Article 49, paragraph 1, second paragraph, reference to the

adequate or appropriate warranties and the means to obtain a copy of these or

to the fact that they have been borrowed.

2. In addition to the information mentioned in section 1, the person responsible for the

treatment will facilitate the interested party, at the moment in which the data is obtained

personal, the following information necessary to guarantee data processing

fair and transparent

a) the period during which the personal data will be kept or, when it is not

possible, the criteria used to determine this period;

b) the existence of the right to request from the data controller access to the

personal data relating to the interested party, and its rectification or deletion, or the limitation

of its treatment, or to oppose the treatment, as well as the right to portability

of the data;

c) when the treatment is based on article 6, paragraph 1, letter a), or article

9, paragraph 2, letter a), the existence of the right to withdraw consent in

any time, without affecting the legality of the treatment based on the

consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

e) if the communication of personal data is a legal or contractual requirement, or a

necessary requirement to sign a contract, and if the interested party is obliged to provide

personal data and is informed of the possible consequences of not

provide such data;

f) the existence of automated decisions, including profiling, to which

referred to in article 22, sections 1 and 4, and, at least in such cases, information

about applied logic, as well as the importance and consequences

provisions of said treatment for the interested party".

Therefore, based on the foregoing, the known facts constitute a

infraction, attributable to the claimed, for violation of article 13 of the RGPD, by not

conveniently inform of the management that was carried out with the personal data

obtained when accessing the community pool.

In this sense, article 72.1.h) of the LOPDGDD, considers it very serious, for

of prescription, “the omission of the duty to inform the affected party about the treatment

of your personal data in accordance with the provisions of articles 13 and 14 of the RGPD”

This infraction may be sanctioned according to the provisions of article 83.5.b) of the

RGPD, where it is established that: “Infringements of the following provisions are

shall be sanctioned, in accordance with section 2, with administrative fines of 20,000,000

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

as a maximum of the overall annual total turnover of the financial year

above, opting for the highest amount: a) the rights of the interested parties to

tenor of articles 12 to 22”.

In accordance with the precepts indicated for the purposes of setting the amount of the penalty

impose, it is considered appropriate to graduate the sanction in accordance with the following

Aggravating criterion established in article 83.2 of the RGPD:

a).- The duration of the infraction, since it is verified, according to the claimant and the

police that the community of neighbors requested the personal data of all those

who, during the summer of 2020, made use of the facilities of the

swimming pool of the community of neighbors (section a).

The balance of the circumstances contemplated in article 83.2 of the RGPD, with

Regarding the infraction committed by violating the provisions of article 13 of the

RGPD, allows you to set a penalty of 3,000 euros, (three thousand euros).

V.- Total Penalty

The balance of the circumstances contemplated in the previous points allows establishing

a total penalty of 6,000 euros (six thousand euros): 3,000 euros for the infringement of the

article 5.1.c) of the RGPD and 3,000 euros for the infringement of article 13 of the RGPD.

In accordance with the foregoing, by the Director of the Spanish Agency for

Data Protection,

RESOLVES:

FIRST: IMPOSE the COMMUNITY OF OWNERS R.R.R., with CIF.:

***NIF.1, the following sanctions:

a).- Penalty of 3,000 euros (three thousand euros) for the infraction of article 5.1.c) of the

GDPR,

b).- Penalty of 3,000 euros (three thousand euros) for the infringement of article 13 of the RGPD,

SECOND: NOTIFY this resolution to the COMMUNITY OF

OWNERS R.R.R.

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

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

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

Common to Public Administrations, within the voluntary payment period indicated in the

Article 68 of the General Collection Regulations, approved by Royal Decree

939/2005, of July 29, in relation to art. 62 of Law 58/2003, of 17

December, by depositing it in the restricted account Nº ES00 0000 0000 0000

0000 0000, opened in the name of the Spanish Agency for Data Protection in the

Bank CAIXABANK, S.A. or otherwise, it will be collected in

executive period.

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

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

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

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

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

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

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure (article 48.6 of the

LOPDGDD), and in accordance with the provisions of articles 112 and 123 of the Law

39/2015, of October 1, of the Common Administrative Procedure of the

Public Administrations, the interested parties may optionally file

appeal for reconsideration before the Director of the Spanish Data Protection Agency

within one month from the day following the notification of this

resolution or directly contentious-administrative appeal before the Chamber of the

Contentious-administrative of the National Court, in accordance with the provisions of the

Article 25 and in section 5 of the fourth additional provision of Law 29/1998, of

July 13, regulatory of the Contentious-administrative Jurisdiction, in the term of

two months from the day following the notification of this act, as

provided for in article 46.1 of the aforementioned legal text.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of Law 39/2015,

of October 1, of the Common Administrative Procedure of the Administrations

Public, the firm resolution may be provisionally suspended in administrative proceedings if

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

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other registers provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Agency for Data Protection.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es