 Procedure No.: PS/00077/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On May 21, 2020, the Agency received a written claim-

tion of D. A.A.A., in which it shows that the website ***URL.1 collects data

but does not comply with the data protection regulations since it is not informed

ma of the person in charge of the file nor is it requested to accept the privacy policy, although

has a legal notice located at the address ***URL.2, it only includes:

“In accordance with the provisions of the Personal Data Protection regulations

Personal, we inform you that you are providing your personal data to the Res-

Responsible for Commercial Treatment of ***URL.1. Contact: Email ***EMAIL.1”..

On May 22, 2020, four claims were received from FACUA in relation to

with the website ***URL.1.

In FACUA's first complaint, the lack of information in the

data Collect. They also claim to have been aware of the existence of

another website ***URL.3 that apparently is directly related to the

denounced website, and this due to the evident similarity between the URL addresses of both

bas pages, as well as in the content of these. On this second website a number is indicated.

mere bank account to make donations.

In the complaint, FACUA provides screen prints made by the entity and Ga-

rant S.L. (company that provides, among other services, tests of the content of

a website at a given time) that certifies the content found on Inter-

net in relation to the address ***URL.1.

The certificates bear the dates of May 20 and 21 along with impressions of

screen of a bank account number to make donations, a confirmation form

touch in which they collect the data of: name, email address, telephone

phone and a message.

Likewise, there is a printout of the "Legal Notice" published on the website in which they report:

“In accordance with the provisions of the Personal Data Protection regulations

Personal, we inform you that you are providing your personal data to the Res-

Responsible for Commercial Treatment of ***URL.1. Contact: Email ***EMAIL.1 and the legislation

estimation of the treatment is based on the consent when clicking the button I ACCEPT THE

DATA PROTECTION POLICY” and printing of the “Terms and conditions”

of the website that includes a data protection section informing

ma ***URL.1 takes the protection of its customers' data very seriously. Is-

do of these General Commercial Terms and Conditions: 05/21/2020 ***URL.1.

In the other complaints, FACUA states that they have verified that on the same platform

In this way, a whole series of documents are archived in which data is collected

personal data of third parties without any kind of protection measure and are found

hosted at the address ***URL.4 accessible by third parties

In this regard, it provides the following addresses where personal data is found-

them:

Emails:

***URL.5

Bank accounts:

***URL.6

***URL.7

***URL.8

Names and surnames and bank accounts:

***URL.9

Names and surnames and other means of payment:

***URL.10

***URL.11

***URL.12

***URL.13

***URL.14

***URL.15

***URL.16

Names and surnames:

***URL.17

They attach screenshots of access to some of these web addresses, cer-

also certified by eGarante, which certify its content as of May 22

of 2020 at 00:57:57 and at 01:02:30. They include personal data, name and

surnames, payment information, proof of payment, bank account numbers.

On the other hand, FACUA indicates that it does not know if those responsible for the

web platform ***URL.1 has been carried out notification to the Agency of the violation in

the security of the personal data that they have archived, as required by the norm

mative.

SECOND: In view of the facts set forth in the claim, the General Subdirectorate

General Data Inspection proceeded to carry out preliminary inspection actions

investigation, having knowledge of the following extremes:

INVESTIGATED ENTITY:

POPULAR RESISTANCE, S.L. with CIF B67580696 and address at ***ADDRESS.1,

***LOCATION.1, (Madrid).

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Previously IYANSA QUALITY SL with CIF B67580696 with address at

***ADDRESS.2 (Barcelona)

RESULT OF THE INVESTIGATION ACTIONS:

On May 25, 2020, the website is accessed from the Data Inspection

***URL.3 verifying that on said website there is a PRIVACY section in which

It consists as responsible for the treatment:

Identity: ***URL.3

Email: ***EMAIL.1

Contact; ***URL.3

Domain name: ***URL.3

Likewise, it is verified that an announcement appears on the web “We will be back in

brief” in which it is reported that “it will remain closed for a few days to

proceed to technical improvements that optimize the shopping experience. All the

orders that have already been placed will be managed and shipped”

On June 9, 2020, the website is accessed from the Data Inspection

***URL.3 verifying the existence of a contact form in which they are requested

the data of: name, email, telephone and message with the following clause: "The

RESPONSIBLE for the treatment is IYANSA QUALITY SL domiciled in C/

***ADDRESS.2, BARCELONA. Purposes: application management, registration, purchase or

query. You can exercise the rights of access, rectification, deletion, portability,

limitation. You can access the remaining information by sending an e-mail to ***EMAIL.1".

Likewise, there is the section "Information on data protection" in which it appears

as the responsible entity IYANSA QUALITY SL. and describing the sections of:

purposes, legal basis, retention period, recipients, rights, type of data

treaties, processes.

On the ***URL.1 website there is a contact form in which the data is requested

from: subject and email address and a box to click the acceptance to

the general conditions and the privacy policy. This website also includes

as responsible IYANSA QUALITY SL.

On June 9, 2020, from the Data Inspection, various

online media:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

 In ***PERIÓDICO.1 dated May 25, 2020, it is reported that FACUA has

denounced the "XXXXXXXX" page for having left the names accessible

name and bank accounts of users

 In ***PERIÓDICO.2 dated May 21, 2020, it is reported that FACUA has

denounced before several organizations to the online store of the Government Resignation

for non-compliance with various electronic commerce regulations, re-

reference to the LOPDGDD and the RGPD.

On June 11, 2020 from the Data Inspection, the urls are accessed

provided by FACUA in its complaint which contained personal data and as

result shows the following message “You don't have permission to access this

resource”.

THIRD: On June 15, 2021, information is requested from IYANSA QUALITY

SL by electronic notification, which had "automatic rejection" as it was not collected by the

entity, which is why a new letter was sent on July 17, 2020.

The response received shows the following:

Regarding the company.

□

IYANSA QUALITY, S.L. has changed its company name and address,

keeping the CIF, being its new denomination POPULAR RESISTANCE

LAR, S.L. and your new address ***ADDRESS.1, ***LOCALITY.1 of Tres

Songs (Madrid).

□ PEOPLE'S RESISTANCE, S.L. has signed a service provision contract

hosting services with SERVYTEC NETWORKS, S.L. dated 29

May 2020 (documents 3, 5 and 6).

□ PEOPLE'S RESISTANCE, S.L. has signed a service provision contract

website maintenance services with SERVYTEC NETWO-

RKS, S.L. dated May 29, 2020. (documents 4 and 7)

Regarding the chronology of the events and actions taken.

□ On June 19, 2020, the Dimitri Government online store opens.

Zion.

□ On June 24, two emails were received from FACUA reporting the ruling.

reason why they close the online store on June 25, after

covering the gap on June 29.

Once detected, proceed to make a modification that prevents the ac-

access to the folders available on the web and the store reopens on July 30

child.

Regarding the causes that made the breach possible.

 POPULAR RESISTANCE manifests the software used (Prestashop- pla-

eCommerce platform that allows you to create online stores) by default it leaves

publish folders with temporary files in which the files are included.

You that users upload through the contact form.

 POPULAR RESISTANCE states that to solve it they modified the

default configuration of the Prestashop from the root files to avoid

to be able to list the folders and the upload of files through

***URL.18.

 PEOPLE'S RESISTANCE, S.L. think it was a human error

scheduling by the data processor, who did not take into account

account the default configuration of Prestashop and was easily corrected.

soon after they detected the fault.

Regarding the affected data.

 POPULAR RESISTANCE states that the number of people affected

there are 6 and the data corresponds to name and surname.

In this regard, it provides a report from the Data Protection Delegate where

of the six documents accessed with personal data of name

and surnames. These documents correspond to some of those provided

by FACUA in its complaint.

 POPULAR RESISTANCE states that it has no knowledge of the use

zation of third parties of the data of the affected people and they only have

proof of access to the data by the complainant FACUA.

Likewise, it states that when doing searches on the Internet, the article does not appear.

goat or data accessed from any of the six people.

In this regard, dated January 18, 2021 from the Inspection of Da-

These have been Google searches of the name and surnames of the

six people affected according to POPULAR RESISTANCE, not finding

proof that the data exists on the Internet is a consequence of the

gap.

 RESISTENCIA POPULAR states that it has notified the bankruptcy at six

people affected and provides a letter stating that "they have been able to

verify the existence of a temporary files folder (which was deleted

mine every 7 days) where the images sent through the

web form. It is there where we have been able to confirm that you

saw an image, being his name and first surname the only data to which

was able to gain access without their permission, noting that the total number of people

affected by the aforementioned reason amounts to 6".

Regarding the security measures implemented before the breach.

 RESISTENCIA POPULAR informs that the security measures are the

adopted by the person in charge of the treatment, referring to those that

they appear on the website ***URL.19 and ***URL.20.

Regarding the measures implemented after the gap.

 RESISTENCIA POPULAR has provided the document "Audit Report.

Record of Personal Data Processing Activities" updated to

dated July 6, 2020 (document 8) in which it appears:

o Record of treatment activities.

o Processing managers and manager and sub-processor model.

o Models for exercising rights.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/13

o Security measures: User management, backup copies,

cookies, organizational measures, training, breach management

Regarding the reason why the breach has not been notified to the AEPD.

 RESISTENCIA POPULAR states that it has not notified as a breach of

security the incident after having carried out the preliminary study of the circumstances

circumstances that accompany what happened and having concluded that it is not a

reportable safety issue, as it is understood that it is not considered a high

risk to the rights and freedoms of the six people affected.

FOURTH: On February 26, 2021, the Director of the Spanish Agency for

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

alleged infringement of article 32 of the RGPD, article 5.1.f) of the RGPD, article 13 of the

RGPD, typified in Article 83.5 of the RGPD.

FIFTH: On April 8, 2021, a resolution proposal was formulated, in which

was proposed,

<<That the Director of the Spanish Agency for Data Protection imposes

IYANSA QUALITY, S.L. with CIF B67580696, a sanction of warning, for

violation of article 5.1.f), in relation to article 5 of the LOPDGDD, as

provided in article 83.5 of the RGPD, considered very serious for the purposes of

prescription in article 72, section 1. i) of the LOPDGDD, for infraction of article

13 in accordance with the provisions of article 83.5, classified as very serious for the purposes of

prescription in article 72 section 1 h) and for violation of article 32 of the RGPD

in accordance with the provisions of article 83.4 of the aforementioned RGPD, classified as serious to

effects of prescription in article 73 section f) of the LOPDGDD. >>

SIXTH: The entity complained against has not submitted arguments to the Proposal for

Resolution.

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

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: A claim is filed for the alleged breach of the regulations

of data protection on the website ***URL.3 and ***URL.1 considering that it is not

would be providing the user with clear and complete information about the treatment of

personal information. In other complaints, FACUA states that they have verified that in

the same platform has a whole series of documents archived in which

collect personal data of third parties without any kind of protection measure and

accessible by third parties.

SECOND: It is stated that on June 24 the security failure was reported, reason

for which they closed the online store the next day, discovering the gap of

security on June 29.

THIRD: The incident has its origin in a programming error. The number of

There are 6 affected people and the data corresponds to name and surname.

FOUNDATIONS OF LAW

Yo

II

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of control, and as established in arts. 47 and 48.1 of the LOPDGDD, the Director of The Spanish Agency for Data Protection is competent to resolve this process.

Article 5.1.f) of the RGPD, Principles related to treatment, states the following:

"1. The personal data will be:

(…)

f) processed in such a way as to ensure adequate security of the data including protection against unauthorized or unlawful processing and against its loss, destruction or accidental damage, through the application of technical measures or appropriate organizational ("integrity and confidentiality").

In the present case, the security breach must be classified as confidential. as a consequence of unauthorized or illicit access to personal data by third parties alien.

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

"1. Those responsible and in charge of data processing, as well as all people who intervene in any phase of this will be subject to the duty of confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary to the duties of professional secrecy in accordance with its applicable regulations.

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

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

treatment".

In the present case, it is proven that personal data of users were

unduly exposed to third parties, violating the principle of confidentiality

established in the aforementioned article 5.1.f) of the RGPD.

III

Article 13 of the RGPD establishes the information that must be provided to the

interested at the time of collection of your personal data:

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

treatment, at the time these are obtained, will provide you with all the information

information indicated below:

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

tant;

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

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 legitimate interests

swindles 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 of adequacy

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

46 or 47 or article 49, section 1, second paragraph, reference to the adequate guarantees

adequate or appropriate and the means to obtain a copy of them or the fact of

that have been borrowed.

2. In addition to the information mentioned in section 1, the data controller

will provide the interested party, at the time the personal data is obtained,

them, the following information necessary to guarantee fair data processing and

transparent:

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

possible, the criteria used to determine this term;

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

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

lien prior to 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 re-

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 providing

tar 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, significant information

tive on applied logic, as well as the importance and anticipated consequences of

said treatment for the interested party.

On the part of this Agency, it has been verified that on the denounced website there is a

contact form in which the data of: name, email, telephone and

message with the following clause: "The RESPONSIBLE for the treatment is IYANSA

QUALITY SL address at C/ ***DIRIMIENTO.2, BARCELONA. Purposes: management of

application, registration, purchase or consultation. You can exercise the rights of access,

rectification, deletion, portability, limitation. You can access the information

remaining by sending an e-mail to ***EMAIL.1".

The collection of personal data through forms included in a page

web page constitutes data processing, for which the person responsible for the processing

The processing must comply with the provisions of article 13 of the RGPD. In this su-

post, it has been found that the website does not provide the user with information

clear and complete information on the processing of your personal data.

IV

Regarding the security of personal data, article 32 of the RGPD "Security

of the treatment", establishes that:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

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

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

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

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular account shall be taken of

takes into account the risks presented by the processing of data, in particular as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The person in charge and the person in charge of the treatment will take measures 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 can only process said data following

instructions of the person in charge, unless it is obliged to do so by virtue of the Right of

the Union or the Member States.

v

The GDPR defines personal data security breaches as “all

those breaches of security that cause the destruction, loss or

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

otherwise, or unauthorized communication or access to such data”.

IYANSA QUALITY, SL has violated article 32 of the RGPD, when there was a breach

security in their systems as a result of a security breach

potentially allowing anyone to access data documents

personal.

It should be noted that the RGPD in the aforementioned precept does not establish a list of the

security measures that are applicable according to the data that are subject

of treatment, but establishes that the person in charge and the person in charge of the treatment

apply technical and organizational measures that are appropriate to the risk involved

the treatment, taking into account the state of the art, the application costs, the

nature, scope, context and purposes of the treatment, the risks of probability

and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and proportionate to the

detected risk, pointing out that the determination of technical measures and

organizational must be carried out taking into account: pseudonymization and encryption,

capacity to guarantee confidentiality, integrity, availability and resilience, the

ability to restore availability and access to data after an incident, process

verification (not audit), evaluation and assessment of the effectiveness of the

measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

"(83) In order to maintain security and prevent the treatment from violating the provisions of

this Regulation, the person in charge or the person in charge must evaluate the risks

inherent to the treatment and apply measures to mitigate them, such as encryption. These

measures must ensure an adequate level of security, including the

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

The responsibility of IYANSA QUALITY, S.L. is determined by the bankruptcy of

security revealed by the claimant, since it is responsible for taking

decisions aimed at effectively implementing technical measures and

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

to ensure the confidentiality of the data and, among them, those aimed at restoring the

availability and access to data quickly in the event of a physical incident or technical. However, the documentation provided shows that the entity failed to comply with this obligation, because the procedures implemented did not prevent that third parties could have the possibility of accessing data that is foreign to them.

Article 83.5 of the RGPD provides the following:

SAW

"5. Violations of the following provisions will be sanctioned, in accordance with the paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, an amount equivalent to a maximum of 4% of the global total annual turnover of the previous financial year, opting for the largest amount:

a) basic principles for treatment, including conditions for consentiment under articles 5, 6, 7 and 9;"

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what following: Violations constitute the acts and conducts referred to in the sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to this organic law.

Establishes article 72 of the LOPDGDD, under the rubric of infractions considered very serious, the following: "1. Based on the provisions of article 83.5 of the Regulation (EU) 2016/679 are considered very serious and will expire after three years infractions that suppose a substantial violation of the articles

mentioned therein and, in particular, the following:

(…)

Yo)

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

this organic law.

For its part, article 72.1.h) of the LOPDGDD considers it very serious, for the purposes 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”

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

serious”, the following:

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

considered serious and will prescribe after two years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the following

following:

(…)

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

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

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

The violation of the principle of confidentiality (art 5.1.f) RGPD) together with the absence

security measures (art 32 RGPD) appropriate to the risk, constitute

the element of guilt that requires the imposition of a sanction.

In the present case, the circumstances provided for in articles 83.5 and 83.4 concur.

of the RGPD and 72.1 i) and h) and 73 f) of the LOPDGDD transcribed above.

7th

Article 58.2 of the RGPD, states the following:

2. Each control authority will have all of the following corrective powers in-

listed below:

(…)

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

when the processing operations have violated the provisions of the

sente Regulation;

viii

Article 70.1 of the LOPDGDD indicates the responsible subjects.

"1. They are subject to the sanctioning regime established in Regulation (EU) 2016/679

and in this organic law:

b) Those responsible for the treatments."

From the foregoing, it is clear that the investigated entity has violated article 5.1.f), in

in relation to article 5 of the LOPDGDD, in accordance with the provisions of article 83.5

of the RGPD, considered very serious for prescription purposes in article 72,

section 1. i) of the LOPDGDD, article 13 in accordance with the provisions of article

83.5, classified as very serious for prescription purposes in article 72 section 1

h) and article 32 of the RGPD in accordance with the provisions of article 83.4 of the aforementioned

RGPD, classified as serious for prescription purposes in article 73 section f) of

the LOPDGD.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE IYANSA QUALITY SL, with CIF B67580696, for a

infringement of Article 32 of the RGPD, Article 5.1.f) of the RGPD, Article 13 of the RGPD,

typified in Article 83.5 of the RGPD, a sanction of warning.

SECOND: NOTIFY this resolution to IYANSA QUALITY SL.

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

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

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

counting from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

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

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the

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

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

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

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es