

□ Procedure No.: PS/00335/2020

RESOLUTION R/00066/2021 TERMINATION OF THE PROCEDURE FOR PAYMENT
VOLUNTEER

In sanctioning procedure PS/00335/2020, instructed by the Spanish Agency for
Data Protection to IDFINANCE SPAIN, S.L., given the complaint filed by
A.A.A., and based on the following,

BACKGROUND

FIRST: On January 14, 2021, the Director of the Spanish Agency for
Data Protection agreed to initiate a sanctioning procedure against IDFINANCE SPAIN,
SL (hereinafter, the claimed party), through the Agreement that is transcribed:

<<

Procedure No.: PS/00335/2020

AGREEMENT TO START A SANCTION PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency and in
based on the following

FACTS

FIRST: A.A.A. (hereinafter, the claimant) dated May 11, 2020
filed a claim with the Spanish Data Protection Agency. The
claim is directed against IDFINANCE SPAIN, S.L. with NIF B66487190 (in
later, the claimed one). The grounds on which the claim is based are as follows:

“The company IDFINANCE SPAIN (MoneyMan), has sent an email of
debt recovery in which it offers a link to make the payment on its website, the
link(**URL.1), does not give me access to my account, but to that of another client, being able to

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/18

apply for loans, consult all your personal data and information related to loans from the entity in question.

I enclose a capture of the data to which I have access, in addition to the email I received,

My biggest concern is that just as I have access to this information that

I must not be able to see so freely, the same thing happens with my personal data and the from other customers.”

Along with the claim, provide the following documents:

1. Mail sent on May 11, 2020 at 5:22 p.m. from the account <***EMAIL.1> to <***EMAIL.2> where you are informed of a balance in favor of MoneyMan and offered various payment methods, among which is the online payment service accessing the link object of the claim.

2. Screenshot of the “Loan History” page of the contract

***CONTRATO.1 where there is a download link for the contract.

3. Screenshot of the “My cards” page where the cards are masked. central numbers of a debit card.

4. Screenshot of the "Contact information" page where the NIE appears, date of birth and email of a person with name and surname

BBB

5. Screenshot of “Address and Employment” page showing address, employment status and information on monthly net income.

SECOND: On May 13, 2020, the Subdirector General for Inspection of Data carried out a verification of the link object of the claim, collecting the following evidence:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/18

1. Download document that contains the Terms and Conditions by which it is governed the loan agreement signed between IDFINANCE SPAIN, S.L. and B.B.B.
2. Printout of page notifying that “[...] your account has been blocked because you do not you meet the requirements to obtain a loan at Moneyman [...]”
3. Printing the “Loan History” page of the contract ***CONTRACT.1.
4. Printing of the “My cards” page where masked numbers appear (except the last 4 digits) of a debit card.

THIRD: In view of the facts denounced in the claim and the documents provided by the claimant, the Subdirector General for Inspection of Data proceeded, on June 3, 2020, to transfer the claim, in accordance with the provisions of article 65.4 of Organic Law 3/2018, of 5 December, of Protection of Personal Data and guarantee of digital rights (in hereinafter LOPDGDD). In this document, the respondent was requested that, within the term of a month to analyze the claim and report on the causes that have motivated the incident that gave rise to the claim, report on the measures adopted to prevent similar incidents from occurring, implementation dates and controls carried out to check its effectiveness.

The respondent filed a reply brief on July 12, 2020 in which states the following:

"[...] FIRST. - Received the claim from that Agency, this entity initiated the investigation of the facts, in the first place, verifying that the systems do not

would have produced any type of security breach that would have given access to personal data from the database.

Said verification was negative and it was verified that there was no fault in the system that would allow a general diffusion of the personal data of the clients.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

4/18

SECOND. - [...]

Once a client registers on the website, their Area is automatically created of User, which can only be accessed through your username and password unique. [...]

[...] when customers default, the agents of the Department of collection initiate the different actions so that the clients comply with the payment of the loan.

One of them is to send, through SMS, never by email, a link to make the payment directly to your User Area, which is what the claimant contributes in the claim.

THIRD. - Received the claim from Mr. A.A.A. proceeded to perform, as has been explained above, an exhaustive investigation-

Once the security breach was ruled out, the investigation of the events described began. in Mr. A.A.A.'s claim.

[...]

This link is generated manually in the system, in the CRM where it is manage customer loans there is the option of sending the SMS with said

link.

We do not know how the claimant was able to receive that link by email

since it is only generated to be sent via SMS. neither have we

been able to carry out the investigation of said mail given that the claimant did not provide it in

the claim.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/18

However, a search has been carried out in the mailboxes

email from which notifications are sent to customers and there is no

email sent neither to the claimant, nor to Mr. B.B.B.

Likewise, a search has been made of all the SMS sent by the

system in the file of Mr. B.B.B. and the only phone number listed is

the one that belongs to said client, so it is technically impossible for that SMS

has been sent to another phone number.

Likewise, we have proceeded to extract from the database all the accesses that were

made to said link, with the IP addresses, the browser and other data, in the

that it is appreciated that, despite the fact that the link has an expiration of 7 days,

accessed it a large number of times, even being opened from the

WhatsApp application.

FOURTH.- Based on the foregoing regarding the facts described by Mr. A.A.A. in

your claim, you did indeed have access to the link sent via SMS to

phone number of Mr. B.B.B. and your User Area, and since IDFinance

Spain S.L.U. scrupulously watches over the data protection rights of the

concerned, proceeded to take measures in order to protect the rights of Mr.

B.B.B., that is, blocking your data in the systems until it can be known

how Mr. A.A.A. had access to that link.

[...] that Agency is requested to require Mr. A.A.A. What does the mail provide?

email you received with that link.

[...]"

The respondent attaches to this document a document listing the accesses to the

link made between April 24, 2020 and May 14, 2020.

FOURTH: The claim was admitted for processing by resolution of the Director

of the Spanish Agency for Data Protection dated September 25, 2020.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/18

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter RGPD) recognizes each

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

The Director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.

II

Article 5 of the RGPD, whose rubric is entitled Principles related to the treatment

establishes in letter f) of its section 1 that personal data will be "processed

in such a way as to ensure adequate security, including protection against

unauthorized or unlawful treatment and against loss, destruction or accidental damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality").

For its part, the LOPDGDD, in its article 5 provides that:

- "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 of the obligor with the person in charge or in charge of the treatment".

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/18

In relation to the measures mentioned in article 5.1.f) of the RGPD before transcribed, article 32 of the same rule provides 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 confidentiality, integrity, availability and resilience

permanent treatment systems and services;

c) the ability to restore the availability and access to the personal data of

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the treatment.

2. When evaluating the adequacy of the security level, particular 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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/18

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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

9/18

III

The claim is based on the alleged security breach in the systems of the claimed that it would have resulted in the provision of a third party of a link that would have freely allowed access to personal data of a identification, location and economic and contractual of another client user and by therefore a violation of the principle of confidentiality in data processing personal by the person responsible for said treatment.

As proof of these statements, the claimant provided the documents to which referred to in the first fact of this agreement.

In this way, the email provided would show that, despite what was stated by the claimed in its letter dated July 12, 2020 in the sense that the link

It is only generated to be sent by SMS, on May 11, 2020 at 5:22 p.m. an email would have been sent from the account <***EMAIL.1> to <***EMAIL.2>. In this email the link ***URL.1 appears as access to the service of online payment of a monetary amount in favor of the claimed.

Likewise, the claimant provides screenshots of the user account to which provides access to the link referred to in the previous paragraph and that does not correspond to yours, but of another person and that allows access to personal data of a identification, location and economic, as well as a link that allows download the signed contract of the client with the claimed. Free access to content of various pages of the user account from the referred link, as well as the possibility of downloading the contract, were confirmed by the checks

made to which reference has been made in the second fact and which were sent as documentation attached to the transfer of the claim sent to the claimant on the day June 3, 2020.

On the other hand, it is pointed out that, according to the list of accesses to the aforementioned link provided by the respondent, it would have been accessed between April 24, 2020 and on May 14, 2020, a period of time clearly greater than 7 days of expiration established for said links indicated by the claimant in his writing.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/18

Taking into account that article 4.12) of the RGPD defines security violations of personal data as “all those security breaches that cause the accidental or unlawful destruction, loss or alteration of personal data transmitted, preserved or treated in another way, or the communication or access is not authorized to said data”, those exposed in the previous paragraphs would show that would have produced a violation of the security measures that would have allowed:

1º That the link had been communicated by a means (email) other than the SMS sent to the customer's mobile phone that, according to what was stated by the claimed constitutes the action procedure.

2º That the link had been active for more than 7 days of expiration declared by the respondent in his answer brief.

3º That it has been possible to freely access, through the aforementioned link, the area of user without the introduction of username and password, so that the claimed indicates as the only way to access said user area

In accordance with the indications available at the present time of agreement to initiate the sanctioning procedure, and without prejudice to what results from the instruction, it is considered that the exposed facts do not comply with what is established in the articles 5.1.f) and 32 of the RGPD, for what they could suppose the commission of paths infractions. The infraction typified in article 5.1.f) is typified in article 83.5 of the GDPR, which provides the following:

“The infractions of the following dispositions 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:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/18

a) the basic principles for the treatment, including the conditions for the consent under articles 5, 6, 7 and 9; [...]

For its part, the infringement of article 32 of the RGPD is typified in article 83.4 of the cited standard, where it is determined that:

“The infractions of the following dispositions will be sanctioned, in accordance with the paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or, in the case of a company, an amount equivalent to a maximum of 2% of the global total annual turnover of the previous financial year, opting for the largest amount:

a) the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 a 39, 42 and 43; [...]"

For the purposes of the limitation period for infringements, article 72.1 of the LOPDGDD, states:

"Based on the provisions of article 83.5 of Regulation (EU) 2016/679, considered very serious and will prescribe after three years the infractions that suppose a substantial violation of the articles mentioned therein and, in particular, the following:

a) The processing of personal data violating the principles and guarantees established in article 5 of Regulation (EU) 2016/679. [...]

And for its part, article 73 of the LOPDGDD, which:

"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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

12/18

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

[...] g) The breach, as a consequence of the lack of due diligence, of the technical and organizational measures that have been implemented in accordance with required by article 32.1 of Regulation (EU) 2016/679. [...]"

v

The corrective powers available to the Spanish Agency for the Protection of Data, as a control authority, is established in article 58.2 of the RGPD. Among

they have the power to sanction with a warning -article 58.2 b)-, the power to impose an administrative fine in accordance with article 83 of the RGPD -article 58.2 i)-, or the power to order the controller or processor that the treatment operations comply with the provisions of the RGPD, when appropriate, in a certain way and within a specified period -article 58. 2 d)-.

According to the provisions of article 83.2 of the RGPD, the measure provided for in article 58.2 d) of the aforementioned Regulation is compatible with the sanction consisting of a fine administrative.

Without prejudice to the provisions of article 83 of the RGPD, the aforementioned Regulation has in its art. 58.2 b) the possibility of sanctioning with a warning, in relation with what is stated in Considering 148:

“In the event of a minor offence, or if the fine likely to be imposed would constitute a disproportionate burden for a natural person, rather than sanction by means of a fine, a warning may be imposed. must however Special attention should be paid to the nature, seriousness and duration of the infringement, its intentional nature, to the measures taken to alleviate the damages suffered, the degree of liability or any relevant prior violation, the manner in which that the control authority has been aware of the infraction, compliance of measures ordered against the person responsible or in charge, adherence to codes of conduct and any other aggravating or mitigating circumstance.”

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

SAW

In the present case, without prejudice to what results from the investigation, they have taken into account

In particular, consider the following elements.

1. As an aggravating circumstance, the connection of the activity of the claimed person with the processing of personal data as that its activity necessarily entails the processing of personal data of the customers (article 76.2.b) of the LOPDGDD).

2. As an extenuating circumstance, the cooperation shown by the claimed with the Spanish Agency for Data Protection in the transfer phase of the claim (article 83.2.f of the RGPD).

For all these reasons, it is considered that the sanctions that should be imposed would be those following:

☐ For the infraction of article 5.1.f) it is considered that the appropriate sanction is that of administrative fine. In this regard, the fine imposed must be, in each individual case, effective, proportionate and dissuasive, in accordance with the provisions of the article 83.1 of the RGPD. Therefore, it is appropriate to graduate the sanction to be imposed in accordance with the criteria established in article 83.2 of the RGPD, and with the provisions of the Article 76 of the LOPDGDD, with respect to section k) of the aforementioned article 83.2 RGPD. In Based on the foregoing, it is considered proportional to set the sanction to be imposed in the amount of five thousand euros (€5,000.00).

☐ For the infraction of article 32, a sanction of warning, in accordance with the established in article 58.2 b) of the RGPD, in relation to what is indicated in the

Considering 148, cited above.

On the other hand, if the existence of infringing conduct is confirmed, it could be agreed impose on the person responsible the adoption of appropriate measures to adjust their actions to the regulations mentioned in this act, in accordance with the provisions of the aforementioned

www.aepd.es

C/ Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

14/18

article 58.2 d) of the RGPD, according to which each control authority may “order the responsible or in charge of the treatment that the treatment operations are comply with the provisions of this Regulation, where appropriate, in a certain manner and within a specified period [...]”.

In such a case, in the resolution adopted, this Agency may require the responsible so that within the period determined:

☐ Certify that you have verified and corrected the implementation of the security measures.

technical, organizational security or both, that avoid the violation of the principle of confidentiality and the making available to third parties of personal data of the customers.

Therefore, in accordance with the foregoing, By the Director of the Agency

Spanish Data Protection, IT IS AGREED:

FIRST: START A SANCTION PROCEDURE against IDFINANCE SPAIN, S.L.,

with NIF B66487190, for the alleged violations of articles 5.1.f) and 32 of the RGPD, typified in articles 83.5 and 83.4, respectively, of the aforementioned standard.

SECOND: APPOINT C.C.C. and secretary to D.D.D., indicating that

any of them may be challenged, where appropriate, in accordance with the provisions of the

Articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the Sector

Public (LRJSP).

THIRD: INCORPORATE to the disciplinary file, for evidentiary purposes, the

claim filed by the claimant and its documentation, as well as the

documents obtained and generated by the Subdirector General for Inspection of Data.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

15/18

FOURTH: THAT for the purposes provided in art. 64.2 b) of Law 39/2015, of 1 October, of the Common Administrative Procedure of the Public Administrations (in hereinafter, LPACAP), the sanction that may correspond for the infraction of article 5.1.f) of the RGPD would be FIVE THOUSAND EUROS (€5,000.00), and by article 32 of the same rule, a WARNING. All this without prejudice to what results from the instruction.

Likewise, the confirmation of the infringing conduct may lead to the imposition of measures in accordance with the provisions of the aforementioned article 58.2 d) of the RGPD.

FIFTH: NOTIFY this agreement to IDFINANCE SPAIN, S.L., with NIF B66487190, granting him a hearing period of ten business days to formulate the allegations and present the evidence it deems appropriate. In his writing of allegations you must provide your NIF and the procedure number that appears in the header of this document.

If within the stipulated period it does not make allegations to this initial agreement, the same may be considered a resolution proposal, as established in article 64.2.f) of the LPACAP.

In accordance with the provisions of article 85 of the LPACAP, in the event that the sanction to be imposed was a fine, it may recognize its responsibility within the term granted for the formulation of allegations to this initial agreement; it

which will entail a reduction of 20% of the sanction to be imposed in the present procedure. With the application of this reduction, the sanction would be set at FOUR THOUSAND EUROS (€4,000.00), resolving the procedure with the imposition of this sanction.

Similarly, you may, at any time prior to the resolution of this procedure, carry out the voluntary payment of the proposed sanction, which will mean a reduction of 20% of its amount. With the application of this reduction, the sanction would be established at FOUR THOUSAND EUROS (€4,000.00) and its payment will imply the termination of the procedure.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

16/18

The reduction for the voluntary payment of the penalty is cumulative with the corresponding apply for the acknowledgment of responsibility, provided that this acknowledgment of the responsibility is revealed within the period granted to formulate arguments at the opening of the procedure. The voluntary payment of the referred amount in the previous paragraph may be done at any time prior to the resolution. In this case, if it were appropriate to apply both reductions, the amount of the penalty would be set at THREE THOUSAND EUROS (€3,000.00).

In any case, the effectiveness of any of the two reductions mentioned will be conditioned to the abandonment or renunciation of any action or resource in via administrative against the sanction.

In case you chose to proceed to the voluntary payment of any of the amounts mentioned above FOUR THOUSAND EUROS (€4,000.00) or THREE THOUSAND EUROS

(€3,000.00), you must make it effective by depositing it into account number ES00 0000

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

Data in the banking entity CAIXABANK, S.A., indicating in the concept the number

reference of the procedure that appears in the heading of this document and

the reason for the reduction of the amount to which it avails itself.

Likewise, you must send proof of payment to the General Subdirectorate of

Inspection to proceed with the procedure in accordance with the quantity

entered.

The procedure will have a maximum duration of nine months from the

date of the start-up agreement or, where appropriate, of the draft start-up agreement.

Once this period has elapsed, it will expire and, consequently, the file of

performances; in accordance with the provisions of article 64 of the LOPDGDD.

Finally, it is pointed out that in accordance with the provisions of article 112.1 of the LPACAP,

There is no administrative appeal against this act.

C/ Jorge Juan, 6

28001 – Madrid

935-200320

www.aepd.es

sedeagpd.gob.es

17/18

Sea Spain Marti

Director of the Spanish Data Protection Agency

>>

: On January 23, 2021, the claimant has proceeded to pay the

SECOND

sanction in the amount of 3,000 euros making use of the two planned reductions

in the Startup Agreement transcribed above, which implies the recognition of the responsibility.

THIRD: The payment made, within the period granted to formulate allegations to the opening of the procedure, entails the waiver of any action or resource in via administrative action against the sanction and acknowledgment of responsibility in relation to the facts referred to in the Initiation Agreement.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of control, and as established in art. 47 of the Organic Law 3/2018, of 5 December, of Protection of Personal Data and guarantee of digital rights (in hereinafter LOPDGDD), the Director of the Spanish Agency for Data Protection is competent to sanction the infractions that are committed against said Regulation; infractions of article 48 of Law 9/2014, of May 9, General Telecommunications (hereinafter LGT), in accordance with the provisions of the article 84.3 of the LGT, and the infractions typified in articles 38.3 c), d) and i) and 38.4 d), g) and h) of Law 34/2002, of July 11, on services of the society of the information and electronic commerce (hereinafter LSSI), as provided in article 43.1 of said Law.

II

Article 85 of Law 39/2015, of October 1, on Administrative Procedure Common to Public Administrations (hereinafter, LPACAP), under the rubric "Termination in sanctioning procedures" provides the following:

"1. Started a sanctioning procedure, if the offender acknowledges his responsibility, the procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction is solely pecuniary in nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature, but the inadmissibility of the second, the voluntary payment by the alleged perpetrator, in any time prior to the resolution, will imply the termination of the procedure, except in relation to the replacement of the altered situation or the determination of the compensation for damages caused by the commission of the infringement.

3. In both cases, when the sanction is solely pecuniary in nature, the competent body to resolve the procedure will apply reductions of, at least,

www.aepd.es

C/ Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

18/18

20% of the amount of the proposed sanction, these being cumulative with each other.

The aforementioned reductions must be determined in the notification of initiation of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of any administrative action or recourse against the sanction.

The reduction percentage provided for in this section may be increased regulations.

In accordance with the above, the Director of the Spanish Agency for the Protection of

Data RESOLVES:

FIRST: TO DECLARE the termination of procedure PS/00335/2020, of in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to IDFINANCE SPAIN, S.L..

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 of the Public Administrations, the interested parties may file an appeal contentious-administrative 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.

Sea Spain Marti

Director of the Spanish Data Protection Agency

936-031219

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es