Procedure No: PS/00206/2022
IMI Reference: A56ID 107954

FINAL DECISION

From the proceedings conducted by the Spanish Data Protection Agency on the basis of the following:

BACKGROUND

FIRST: [redacted] (hereinafter the complainant) lodged a complaint with the Dutch Data Protection Authority. The complaint is directed against BANKINTER, S.A. with VAT A28157360 (hereinafter BANKINTER). The grounds on which the complaint is based are as follows:

The complainant exercised his right of access to BANKINTER and received a reply on 4 February 2019 stating that he was not registered as a customer or a former customer.

Together with the complaint he provided:

— Copy of an email from the complainant to *privacidad@bankinter.com*, dated 29 January 2019, in which he attached his request for access to his personal data in PDF.

— Copy of an email from *privacidad@bankinter.com* to the complainant, dated 31 January 2019, informing him that his request has been forwarded to the relevant department, from which it will be provided with a reply within the prescribed time limit and form.

— Copy of an email from the complainant to privacidad@bankinter.com, dated 12 February 2019, informing: "Good afternoon, I received your reply by post today (attached), in which you refuse to have any product contracted with me, please note that this is not true, as I have an open account with you [redacted]). Please find attached a document issued by you with reference to this account. I therefore ask you to review your records again and proceed with the request. Regards'

— Copy of an email *from* privacidad@bankinter.com to the complainant, dated 14 February 2019, informing the complainant: 'We forward your request to the relevant department, from which you will be answered within the prescribed time-limit and form.*'*

— Copy of a document from BANKINTER dated September 2017 addressed to the complainant, in which it is sent the information relating to his transactions with Bankinter, which is necessary to complete his tax return for the financial year 2016, stating that the complainant is the holder of the account number [redacted]

— Copy of a document signed by the complainant, dated 29 January 2019, requesting BANKINTER to have access to his personal data.

— Copy of a BANKINTER document dated 4 February 2019 addressed to the complainant, informing him that they are unable to comply with his request for access since his data are not included in their records as a client or former customer of the entity.

SECOND: Via the 'Internal Market Information System' (IMI), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), the purpose of which is to promote cross-border administrative cooperation, mutual assistance between the Member States and the exchange of information, the Spanish Data Protection Agency (AEPD) received the aforementioned complaint on 7 February 2020. This complaint is forwarded to the AEPD in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter GDPR), taking into account its cross-border nature and the fact that this Agency is competent to act as lead supervisory authority, given that BANKINTER has its registered office and single establishment in Spain.

According to the information incorporated into the IMI system, in accordance with Article 60 of the GDPR, it acts as a 'supervisory authority concerned', in addition to the data protection authority of the Netherlands, the Portuguese authority. The latter under Article 4 (22) of the GDPR, since data subjects residing in that country are likely to be substantially affected by the processing which is the subject of the present proceedings.

THIRD: On 3 July 2020, in accordance with Article 64 (3) of Spanish Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), the complaint lodged by the complainant was declared admissible.

FOURTH: The General Subdirectorate for Data Inspection carried out preliminary investigations to clarify the facts in question, in accordance with the tasks assigned to the supervisory authorities in Article 57 (1) and the powers conferred on them by Article 58 (1) of Regulation (EU) 2016/679 (GDPR), and in accordance with the provisions of Title VII, Chapter I, Section 2, of the Spanish LOPDGDD, taking note of the following:

In response to a request for information from this Agency on 30 April 2020, the representatives of BANKINTER stated that they had adequate procedures and mechanisms in place to comply with the data protection rights of data subjects. They provide a copy of the procedure.

In relation to the reason why the reply provided to the complainant as a result of his exercise of the right of access which did not contain information relating to account [redacted] the representatives of the complainant indicate that there was a one-off error in the application of the Rights Procedure. As a result, the account was not located and identified as corresponding to the complainant, so Bankinter did not provide him with such information.

On 20 April 2020, the error was resolved and the complainant's right of access was answered in full. The entity's representatives provide a copy of the email sent to the complainant with the information requested in an encrypted attachment, the key of which is his identity card.

FIFTH: On 25 April 2022, the Director of the AEPD declared the proceedings time-barred, since more than 12 months had elapsed since the date on which the complaint was declared admissible, thus a new investigation was opened under number AI/00170/2020, and the documentation contained in E/02670/2020 was added to this new investigation.

SIXTH: On 28 June 2022, the General Subdirectorate for Data Inspection of this Agency made a screenshot on the website https://monitoriza.axesor.es/, relating to the size and turnover of BANKINTER S.A., which does not find information on the last financial year submitted (2021), but which is recorded as a group parent company with a share capital of 269.659.846 EUR.

SEVENTH: On 1 July 2022, the Director of the AEPD adopted a draft decision to initiate penalty proceedings. Following the process set out in Article 60 GDPR, this draft decision was transmitted via the IMI system on 5 July 2022 and the authorities concerned were informed that they had four weeks from that time to raise relevant and reasoned objections. The time limit for handling these penalty proceedings was automatically suspended for these four weeks, in accordance with Article 64.4 of the Spanish LOPDGDD.

Within the deadline for that purpose, the CSAs did not raise any relevant and reasoned objections to it, and therefore all authorities are deemed to agree with and are bound by that draft decision, in accordance with Article 60(6) GDPR.

This draft decision was notified to BANKINTER on 11 July 2022, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

EIGHTH: On 30 January 2023**,** the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against BANKINTER in order to impose a fine of 1,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP), for the alleged infringement of Article 15 of the GDPR, as defined in Article 83 (5) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was not collected by BANKINTER within the time limit for making it available, so it was deemed to have been rejected in accordance with Article 43.2 of the LPACAP on 12 February 2023, as stated in the certificate contained in the file.

NINTH: On 24 February 2023, BANKINTER submitted a letter to this Agency explaining that it had become aware, via the Authorised Electronic Directorate (DEH), that the AEPD made available to Bankinter S.A a notification and that it is in a situation of 'Rejected'. However, on this occasion, no notification had been received from the AEPD informing Bankinter S.A of making a notification available on the website Authorised Electronic Address (DEH) or in the Single Authorised Electronic Address (DEHu), a practice which is common practice on the part of the Agency. The reason for the rejection was therefore that Bankinter had not been aware that it had a notification in the

Authorised Electronic Directorate. It therefore requested that that notification be sent back to Bankinter so that it could have access to the content of the notification and put forward the relevant arguments and, where appropriate, propose evidence which it considers relevant.

On 28 February 2023, the Agency made available to Bankinter via electronic means a copy of the agreement to initiate these penalty proceedings, which was duly collected on the same day, as stated in the acknowledgement of receipt in the file.

TENTH: On 9 March 2023, this Agency received a letter from BANKINTER, in due time and form, in which BANKINTER put forward arguments relating to the decision to initiate the procedure in which it stated that BANKINTER had acted unintentionally and that the penalty was not proportionate, given that there were mitigating factors that had not been taken into account and that the aggravating factors considered in the decision to initiate the procedure should not be such. It requested that the present penalty proceedings be discontinued or, in the alternative, that a reprimand be issued to it or, failing that, a minimum fine should be imposed on it.

ELEVENTH: On 21 March 2023**,** the person handled the proceedings adopted a proposal for a resolution in which it is proposed to the Director of the Spanish Agency of the Spanish Data Protection Agency to impose a fine of 1,000 EUR to BANKINTER, for the alleged infringement of Article 15 of the GDPR, as defined in Article 83 (5) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

TWELFTH: On 28 March 2023, BANKINTER paid the penalty.

The payment made entails the waiver of any action or appeal against the final decision, in relation to the facts referred to in the proposal for a resolution.

From the handling of this procedure and from the documentation in the file, there have been established the following:

PROVEN FACTS

FIRST: On 29 January 2019, the complainant sent an email to *privacidad@bankinter.com,* enclosing his request for access to his personal data in PDF.

SECOND: On 31 January 2019, the complainant received an email from privacidad@bankinter.com informing him that his request has been forwarded to the relevant department, from which he will be provided with a reply within the prescribed time limit and form.

THIRD: On 4 February 2019, BANKINTER addressed a document to the complainant informing him that they are unable to comply with his request for access as his data are not included in their records as the entity's customer or former customer.

FOURTH: On 12 February 2019, the complainant sent an *email* to privacidad@bankinter.com informing: "Good afternoon, I received your reply by post

today (attached), in which you refuse to have any product contracted with me, please note that this is not true, as I have an open account with you [redacted] Please find attached a document issued by you with reference to this account. I therefore ask you to review your records again and proceed with the request. Regards'.'

Together with this email, the complainant provides a copy of a document from BANKINTER dated September 2017 addressed to the complainant, which sends him the information relating to his transactions with Bankinter, which is necessary to complete his tax return for the financial year 2016, stating that the complaining holds account number [redacted]

FIFTH: On 14 February 2019, the complainant received an *email from privacidad@bankinter.com* informing it: 'We forward your request to the relevant department, from which you will be answered within the prescribed time-limit and form.*'*

SIXTH: On 20 April 2020, BANKINTER replied to the complainant's right of access, by email sent to the complainant with his personal data by means of an encrypted attachment, the key of which was ***his identity card***.

LEGAL GROUNDS

I
Competence

In accordance with the powers conferred on each supervisory authority by Article 58 (2) and (60) of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter 'the GDPR'), and in accordance with Articles 47, 48.1, 64.2 and 68.1 of Spanish Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is competent to initiate and decide on this procedure.

In addition, Article 63 (2) of the Spanish LOPDGDD states that: 'The *procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this Organic Law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures.*'

II
Preliminary remarks

In the present case, in accordance with Article 4 (1) of the GDPR, there is a processing of personal data, since BANKINTER collects and stores, inter alia, the following personal data of natural persons: first name, surname, address and e-mail address, among other processing.

BANKINTER carries out that activity in its capacity as controller, since it is the person who determines the purposes and means of that activity, pursuant to Article 4 (7) of the GDPR. Moreover, it is a cross-border processing, given that BANKINTER is established in Spain, although it provides services to other countries of the European Union.

Article 56 (1) of the GDPR provides, for cases of cross-border processing, provided for in Article 4 (23) thereof, in relation to the competence of the LSA, that, without prejudice to Article 55, the supervisory authority of the main establishment or the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60. In the case examined, as explained above, BANKINTER has its sole establishment in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

For its part, the right of access to personal data is governed by Article 15 of the GDPR.

III
Allegations

With regard to the allegations to the decision to initiate these penalty proceedings, we will respond to them in the order set out by BANKINTER:

1.- LACK OF INTENTIONALITY AND FAULT IN BANKINTER'S ACTIONS

BANKINTER claims that its reply to the complainant was due to a human error, which was only noticed when the AEPD sent the request for information to this entity.

And that the incident described – which is clearly unfortunate – should be regarded as one-off and isolated; something almost fortuitous which 'escaped' the measures and remedies available to Bankinter for the management of data subjects' rights.

It indicates that:

(a) Bankinter had and has in place appropriate technical and organisational measures to address data subjects' rights in the strictest respect of the GDPR, its principles and obligations. In particular, in the reply to the request, the Rights Procedure was provided as Document No 1.

According to BANKINTER, this procedure is considered to be effective. And that Bankinter is not in vain a financial institution which receives on average more than 44 applications for allowances per month (reaching 83 applications in January and February 2023). However, even taking into account the huge number of applications that the entity has been receiving and managing since 2018, only twelve have resulted in actions before the AEPD. It should be pointed out that, apart from the present case, the rest have ended either in the closure of proceedings or in the rejection of the complaint by the AEPD. Those figures merely show how robust Bankinter's procedures and the entity's great diligence are.

In any event, it states that:

(b) Bankinter had and has a specialised department responsible for replying to all requests for data subjects' rights. Having a department that only deals with replies to rights ensures that they are answered in due time and form. This department works in conjunction with legal advice on non-operational issues.

(c) Bankinter argues that there is absolute traceability of the exercise of rights by the data subjects. All applications received through any channel are managed via a software application and there is also a procedure in place to ensure the correct management of the rights exercised.

(D) It also points out that all employees of Bankinter are required to comply with data protection obligations, in which, inter alia, for the purposes of the present case, they are informed of the importance of responding correctly and in due time to requests for data protection rights.

In this respect, this Agency would like to point out that it is not the subject of this procedure to assess the procedure that BANKINTER might have put in place for the purposes of the exercise of rights, but rather to assess whether BANKINTER duly responded to the complainant's request for access rights, in accordance with the provisions of the GDPR.

1.5. However, BANKINTER argues that as is generally the case with any procedure; the measures and controls described, although robust, are not infallible, being the event (they insist, isolated and one-off) occurred with the complainant, the evidence and the consequence of this.

1.6. In that regard, and in addition to what has been stated, it points out and stresses that the Bankinter's procedures to minimise the consequences of errors which, as in the present case, may occur, present solutions to them quickly and effectively. Thus, in the present case, even in the midst of the COVID-19 pandemic, Bankinter, on 20 April 2020, responded and satisfied the complainant's right as soon as it became aware of the situation after receiving the request from the AEPD.

In this regard, this Agency would like to point out that responding to the request to exercise the right of access to the complainant is nothing other than to comply with the provisions of the GDPR.

1.7. BANKINTER states that a clearly isolated and punctual error (there is no better evidence of this than the fact that no further complaints have been lodged in this regard or by indicating this type of error), such as that in the present case – which, even though it is formalised, reviewed, managed and automated, is impossible to avoid in absolute terms – must not deny the proper diligence which Bankinter has when faced with the exercise of rights by the data subjects, which is measured and confirmed by its usual and daily behaviour and the existence of policies, controls and responsiveness as described above.

In this respect, the Agency would like to point out that the fact that there were no further complaints or "indicating this type of error" does not conclude a proof that this is "a clearly isolated and one-off error", but it is not the subject of the present procedure to assess

only whether in the case of the complainant BANKINTER duly responded in due time and form to the request for the exercise of the right of access in question.

1.8. BANKINTER argues that the proper contextualisation of the event with the complainant and its assessment of an isolated error with regard to the procedures and controls implemented by Bankinter is not a balantal issue, since it makes it possible to dissociate such an event from a wrongful conduct on the part of Bankinter, without which there can be no sanction.

1.9. Indeed, as has been recognised by settled case-law, the principles underlying the criminal order apply, with certain nuances, to administrative law imposing penalties (for all, Judgment of the Constitutional Court – 'STC' – No 18/1981). The principle of guilt also applies to administrative offences and its system of penalties, as a manifestation of the State's ius puniendi. A system of strict or no-fault liability is therefore inadmissible in our legal order (STC No 76/1990).

In this regard, Article 28.1 of Law 40/2015 of 1 October on the Legal Regime for the Public Sector ('LRJSP') expressly states that:

'Only natural and legal persons and, where a law grants them capacity to act, groups of persons affected, unions and entities without legal personality and independent or autonomous assets, which are responsible for them intentionally or negligently, may be penalised for acts constituting an administrative offence'.

In other words, without proven negligence or wilful misconduct, it cannot be held liable for an infringement.

1.10. BANKINTER states that it could perhaps be argued that it had to be negligent because otherwise the mistake would not have been committed which, in turn, was inadequately attentive to the complainant's right. However, it believes such an allegation should also be rejected as it is not acceptable in our right to impose penalties.

1.11. BANKINTER states that a one-off and extraordinary error (as in the present case) does not in itself permit the inference of the existence of wrongful conduct. This would mean the definitive objectivity of the fault, where the result is equivalent to the subjective element (proscribed structure in our criminal or administrative law).

1.12. In these terms, the National High Court has ruled on a number of judgments: an isolated error cannot in itself give rise to liability where it is not intentionally or negligent and the appropriate diligence has been exercised. For all, the judgment of the National High Court of 23 December 2013 (Rec. 341/2012) (which, moreover, is cited by the AEPD itself in numerous decisions applying this doctrine – for example, those in cases E/05498/2017, E/06654/2017 or E/00878/2018 –) states in this regard that:

'The question must therefore be resolved in accordance with the principles specific to punitive law, since mere human error cannot lead, in itself (and above all when it occurs in isolation), to the imposition of penalties; if so, there would be a system of strict liability that is prohibited by our constitutional order.

In the field of the protection of personal data, in order for such an error to be relevant for punitive purposes, it must be the consequence – or be possible – of the absence of prior and adequate control procedures aimed at preventing it.

Only in that way will there be a fault factor in the company, which can be attributed to recklessness (or 'mere non-compliance') due to failure to articulate protocols or security procedures. However, those deficiencies must be investigated and proved by the administrative penalty body (which bears the burden of doing so in order to destroy the presumption of innocence).
(...)

In the present case, however, none of this is stated in the decision imposing a penalty, nor does it serve to support the conclusion that, if the error occurred, it is because the security protocols were not established or insufficient. This would be a false and controversial conclusion with the fallible human dimension.

It is therefore not a question of ensuring the absence of errors by means of punitive law, but of organising procedures for pre-damage, and then also of sanctioning if those protocols are not established or are insufficiently established'.

In this respect, this Agency would like to point out that the present case is not a one-off error or an isolated error, which alone gives rise to liability without any fault or wilful misconduct on the part of BANKINTER.

To deny that BANKINTER acted negligently would be tantamount to recognising that its conduct – by action or omission – was diligent. Obviously, this perspective of the facts is not shared, as a lack of due diligence has been established. A large company that routinely processes its customers' personal data, such as BANKINTER, must take utmost care to comply with its data protection obligations, as established by the case-law. It is very illustrative that the SAN of 17 October 2007 (rec. 63/2006), assuming that these are entities whose activity involves continuous processing of customer data, states that '... the Supreme Court has taken *the view that there is recklessness whenever a legal duty of care is disregarded, that is to say, where the offender does not act with the requisite diligence. In the assessment of the degree of diligence, particular consideration must be given to the professionalism or otherwise of the data subject, and there is no doubt that, in the present case, when the appellant's activity is constant and abundant in the handling of personal data, emphasis must be placed on rigour and exquisite care because it complies with the legal provisions in this regard'.*

In the present case, the complainant sent a first email on 29 January 2019 requesting access to his personal data. Bankinter replied that it could not provide him with such data because he did not count as a customer or former customer of the bank.

However, the complainant sent a second email on 12 February 2019 indicating to the bank that he was a customer and attached a number of documents proving that situation. And this second email received no reply from the bank.

In other words, the complainant contacted the bank again so that it could correct the initial reply, but the bank did not give due consideration to this request, even after the

complainant had provided the relevant documentation to enable the bank to remedy the situation.

The fact that BANKINTER did not provide a proper response to the complainant once again contacted the bank in order to remove it from its error in its first reply demonstrates the lack of due diligence that could be expected from a bank in the category of BANKINTER, which continuously processes its customers' personal data.

1.13. BANKINTER argues that the Agency itself has closed complaints on the basis of that fact, a one-off error cannot amount to wrongful conduct resulting in administrative liability. As an example, the decision to close proceedings in Case E/06894/2020, where the AEPD acknowledges that:

'it is established that the action of the requested person as a controller, although it infringed the provisions of the data protection legislation by including the address of the notified person, which was due to a specific error, has already put in place the necessary measures to ensure that the facts at issue in this complaint do not recur.'

In that regard, the Agency wishes to point out that procedure E/06894/2020 is a substantially different situation, since it is not even an exercise of rights but an unauthorised dissemination of personal data. In that procedure, it was decided to close the proceedings on the basis that it was a one-off error which was corrected or known to it and that measures were put in place to prevent such a situation from happening again, both of which do not arise in the present case, since the bank did not give due reply to the complainant in so far as it made known that it was a customer and had to provide him with the information in its possession, nor has it been established that the bank had taken measures to prevent a similar situation from recurring in the future.

1.14. In addition, BANKINTER claims that, as soon as it became aware of the error, it proceeded to resolve it and give the complainant access to the data requested, demonstrating that it had adequate mechanisms in place to deal effectively with an incident such as that which occurred. All this cannot be overlooked by the AEPD when analysing Bankinter's guilt (in reality, lack of guilt) in the present case.

In this regard, the Agency reiterates that BANKINTER was informed of its error by the complainant in his email of 12 February 2019, in which he stated not only that he was a client but also provided the relevant documentation to prove such a situation, and thus to be able to obtain access to his data, as he had previously requested, but this email was not duly answered. Access was given to the complainant's data once this Agency requested BANKINTER to provide information on this issue.

1.15. BANKINTER argues that AEPD itself took account of this type of circumstances in decisions such as that given in Case PS/00019/2021, in which there was no guilt, as detailed below:

'In the present case, it is common ground that the requested person, once it became aware of the errors that were occurring in the cross-checking of data with the Robinson list of Adigital, acted with due diligence by correcting the error detected by sending on 5/02/2020 a new corrected list to the one under investigation and by adding to its internal list the numbering that is the subject of the complaint, ceasing the calls to the complainant

henceforth. Consequently, the fact that the conduct initially alleged was guilty is not assessed by the person under investigation.'

In that regard, the Agency wishes to point out that procedure PS/00019/2021 is a substantially different situation, since it is not even an exercise of rights but the making of advertising calls once the right to object had been exercised, nor is it an infringement of the GDPR but of Law 9/2014 of 9 May 2003, General Law on Telecommunications. In those proceedings, it was decided to close the proceedings on the ground that the error in the cross-checking of data with the Robinson list of Adigital was due to a specific error in the system for filtering numerations with the Robinson list of Adigital, there was no fault in its conduct, since it was due to a change in the system for filtering the Robinson numerations of Adigital during the period from 2020 to February 2021, and that the alleged error, before becoming aware of the impact on downloads of the Robinson List of Adigital, proceeded to diligently correct that error, as is apparent from the chronology of the facts and the content of the administrative file, which is why the conduct initially imputed to the defendant lacks any element of guilt as it resulted from an error and, consequently, the defendant is not liable for the acts initially imputed.

However, in the present case, this is not an error resulting from a change outside the control of BANKINTER, nor did BANKINTER act with the due diligence which it was required, since it did not respond properly to the complainant's request, even when he had provided it with the information relating to the fact that he was a customer.

1.16. BANKINTER argues that, in other proceedings, such as E/06746/2020, the AEPD closed the proceedings on the grounds that the complainant had reasonable measures to prevent errors and to act expeditiously to update them as the entity realised that they were not sufficient:

'It appears from the investigation that [redacted] *had preventive technical and organisational measures in order to avoid this type of incident, however, the incident now analysed.*
(...)
the entity under investigation had reasonable technical and organisational measures to prevent this type of incident and which, as they prove to be insufficient, have been updated expeditiously."

In this regard, the Agency wishes to point out that procedure E/06746/2020 is a substantially different situation, since it is not even an exercise of rights but a personal data breach. In that procedure, it was decided to close the proceedings on the basis that the entity under investigation had reasonable technical and organisational measures to prevent this type of incident and that, as they prove to be insufficient, they have been updated diligently, which is not the case in the present case, since the bank did not acted with due diligence in providing an answer to the complainant as soon as he informed that he was a customer and had to provide him with the information it had, nor has it been established that the bank had taken measures to prevent a similar situation from recurring in the future.

1.17. BANKINTER argues that, since the inadequate attention of the complainant's right of access was due to a one-off error and not to a negligent conduct on the part of

Bankinter, the AEPD must close the present sanctioning proceedings on the ground that the element of fault was not present.

In this regard, we would reiterate that to deny that BANKINTER acted negligently would be tantamount to recognising that its conduct – by action or omission – was diligent. Obviously, this perspective of the facts is not shared, as a lack of due diligence has been established. A large company that routinely processes its customers' personal data, such as BANKINTER, must take utmost care to comply with its data protection obligations, as established by the case-law. It is very illustrative that the SAN of 17 October 2007 (rec. 63/2006), assuming that these are entities whose activity involves continuous processing of customer data, states that '... the Supreme Court has taken *the view that there is recklessness whenever a legal duty of care is disregarded, that is to say, where the offender does not act with the requisite diligence. In the assessment of the degree of diligence, particular consideration must be given to the professionalism or otherwise of the data subject, and there is no doubt that, in the present case, when the appellant's activity is constant and abundant in the handling of personal data, emphasis must be placed on rigour and exquisite care because it complies with the legal provisions in this regard'.*

In the present case, the complainant sent a first email on 29 January 2019 requesting access to his personal data. Bankinter replied that it could not provide him with such data because he did not count as a customer or former customer of the bank.

However, the complainant sent a second email on 12 February 2019 indicating to the bank that he was a customer and attached a number of documents proving that situation. And this second email received no reply from the bank.

In other words, the complainant contacted the bank again so that it could correct the initial reply, but the bank did not give due consideration to this request, even after the complainant had provided the relevant documentation to enable the bank to remedy the situation.

The fact that BANKINTER did not provide a proper response to the complainant once again contacted the bank in order to remove it from its error in its first reply demonstrates the lack of due diligence that could be expected from a bank in the category of BANKINTER, which continuously processes its customers' personal data.

In the light of the foregoing, the present allegation is rejected.

2. — IN THE ALTERNATIVE, ON THE NECESSARY PROPORTIONALITY OF THE PENALTIES AND THEIR SCALE. APPLICATION OF MITIGATING FACTORS AND ABSENCE OF AGGRAVATING CIRCUMSTANCES.

2.1. In the alternative to the First Allegation, in the unlikely event that Bankinter is held liable for the infringement of Article 15 on the basis of some sort of fault (quod non), BANKINTER argues that the Agency must take into account the following mitigating circumstances (which it excludes in the Initiation Agreement without going to analyse them), in order to determine the amount of the fine and the imposition of the reprimand, in accordance with Articles 83.2 GDPR and 76.2 of the LOPDGDD:

(a) The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them (Art. 83.2.a GDPR)

In the present case, the situation has led to a late response to the exercise of a single person's right of access due to a one-off error.

The provisions of Article 83.2.a) GDPR can only be understood as applying to this case as an attenuating circumstance.

In this respect, this Agency would like to point out that it is not a question of BANKINTER having given a 'late response' to the complainant, but rather that the bank had not replied in any way to the complainant and was only given access after the complaint had been declared admissible and after it had been requested to provide information on the case.

According to the judgment of the National High Court SAN 3432/2009, *'the failure to reply to the complainant's requests for access and their delivery to another company constitutes an obstacle to the right of access granted to everyone affected by Article 15 of the LOPD, and which Article 44 (3) (e) classifies as a serious infringement'*. In other words, the failure to provide access to the complainant to the data held by BANKINTER is an obstacle to the right of access.

For that reason, such a situation cannot be regarded as an attenuating situation, but rather the opposite. The present allegation is therefore rejected.

(b) the intentional or negligent character of the infringement (Art. 83.2.b GDPR)

BANKINTER claims that it has acted with due diligence, implementing pre- and post-spot error measures, in a preventive and proactive manner to ensure the protection of the personal data it processes, and to respond properly to the rights. In the rare assumption that the AEPD considers that there is guilt, it has been established that this circumstance must be understood as a mitigating factor.

In this regard, we would reiterate that to deny that BANKINTER acted negligently would be tantamount to recognising that its conduct – by action or omission – was diligent. Obviously, this perspective of the facts is not shared, as a lack of due diligence has been established. A large company that routinely processes its customers' personal data, such as BANKINTER, must take utmost care to comply with its data protection obligations, as established by the case-law. It is very illustrative that the SAN of 17 October 2007 (rec. 63/2006), assuming that these are entities whose activity involves continuous processing of customer data, states that '... the Supreme Court has taken *the view that there is recklessness whenever a legal duty of care is disregarded, that is to say, where the offender does not act with the requisite diligence. In the assessment of the degree of diligence, particular consideration must be given to the professionalism or otherwise of the data subject, and there is no doubt that, in the present case, when the appellant's activity is constant and abundant in the handling of personal data, emphasis must be placed on rigour and exquisite care because it complies with the legal provisions in this regard'.*

In the present case, the complainant sent a first email on 29 January 2019 requesting access to his personal data. Bankinter replied that it could not provide him with such data because he did not count as a customer or former customer of the bank.

However, the complainant sent a second email on 12 February 2019 indicating to the bank that he was a customer and attached a number of documents proving that situation. And this second email received no reply from the bank.

In other words, the complainant contacted the bank again so that it could correct the initial reply, but the bank did not give due consideration to this request, even after the complainant had provided the relevant documentation to enable the bank to remedy the situation.

The fact that BANKINTER did not provide a proper response to the complainant once again contacted the bank in order to remove it from its error in its first reply demonstrates the lack of due diligence that could be expected from a bank in the category of BANKINTER, which continuously processes its customers' personal data.

In the light of the above, this claim is rejected.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects (Art. 83.2 (c) GDPR)

BANKINTER argues that when it became aware of the error in the reply, it responded to the complainant's right of access without any further damage due to the delay in the reply. That must also be taken into account as an attenuating circumstance.

In this regard, the Agency reiterates that BANKINTER was informed of its error by the complainant in his email of 12 February 2019, in which he stated not only that he was a client but also provided the relevant documentation to prove such a situation, and thus to be able to obtain access to his data, as he had previously requested, but this email was not duly answered. Access was given to the complainant's data once this Agency requested BANKINTER to provide information on this issue. That, moreover, was nothing other than their obligation.

The present allegation is therefore rejected.

(D) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement (Art. 83.2 (f) GDPR)

In line with what was stated above, BANKINTER claims that it took the appropriate measures to remedy the situation, which it duly informed the Agency in its reply to the request. Bankinter cooperated in good faith with the AEPD to remedy the infringement and in fact succeeded in doing so, which must be taken into account as an attenuating circumstance.

In this regard, we would like to point out that replying to the requests for information it makes is a legal obligation under Article 52 of the LOPDGDD, which provides that: '*Public Administrations, including tax and social security administrations, and individuals*

shall be obliged to provide the Spanish Data Protection Agency with data, reports, background and proofs necessary for carrying out their investigation activities'. It was therefore an obligation on BANKINTER to provide this information to this Agency.

In the light of the above, this allegation is rejected.

2.2. BANKINTER argues that the present case should not entail the imposition of a fine, but in any event a reprimands (AEPD's power under Article 58.2 (b) of the GDPR). This, according to recital 148 GDPR, can be imposed on the basis of:

'In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor.'

It states that, in the present case, there is no doubt that there is a minor infringement, and the fact that it is classified as 'very serious' for the purposes of limitation alone cannot change that consideration.

In this regard, the Agency would like to point out that the requirements set out in recital 148 of the GDPR are not met, since this is not a minor infringement for the purposes of the GDPR, since this is the obstacle to the complainant's exercise of the right of access due to BANKINTER's lack of due diligence, nor is it a penalty directed against a natural person. The present claim is therefore rejected.

2.3. The failure to take account of the abovementioned mitigating measures, and the resulting reduction in the proposed amount or the imposition of a reprimand, would make the amount currently proposed entirely contrary to the principle of proportionality governing the administrative penalty procedure in relation to the infringement in question, resulting in a disproportionate penalty (however small).

In this respect, the Agency reiterates the above and rejects this allegation.

IV
Right of access

Article 15 '*Right of access by the data* subject' of the GDPR provides:

'1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others'.

In the present case, it is common ground that the complainant had requested BANKINTER to have access to his personal data by email on at least two occasions. The last time, on 12 February 2019, when he informed the bank that he was a customer and provided the relevant documentation to prove that fact.

For its part, BANKINTER replied to him for the first time that it did not have his data and the second time sent him an email only to the complainant informing him that his request had been forwarded to the relevant department, from which it would be able to respond within the prescribed time limit and form. However, the complainant did not receive any subsequent reply until, after receiving a request for information from this Agency, it was granted access to the requested information on 20 April 2020. This is more than one year after having requested it and only after the intervention of this Agency.

In accordance with the evidence available at this stage, we consider that the known facts constitute an infringement, attributable to BANKINTER, of Article 15 of the GDPR.

V

Classification of the infringement of Article 15 of the GDPR

The aforementioned infringement of Article 15 of the GDPR lead to the commission of the infringements referred to in Article 83 (5) of the GDPR, which, under the heading *'General conditions for imposing administrative fines'*, provides:

'*Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*

(…)

(b) the data subjects' rights pursuant to Articles 12 to 22;'

In that regard, Article 71 (*'Infringements'*) of the Spanish LOPDGDD provides that:

'The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements.'

For the purposes of the limitation period, Article 72 '*Very serious infringements'* of the Spanish LOPDGDD states:

'In accordance with article 83.5 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered very serious infringements and its limitation period shall be three years:

(...)

[k) The obstacle or hindrance to or repeated failure to exercise the rights foreseen in articles 15 to 22 of Regulation (EU) 2016/679 (...)'

VI
Sanction

This infringement may be fined up to EUR 20.000.000 or, in the case of an undertaking, up to 4 % of the total total annual turnover of the preceding financial year, whichever is higher, in accordance with Article 83 (5) of the GDPR.

Furthermore, for the purposes of deciding on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage, it is considered that the balance of the circumstances referred to in Article 83 (2) of the GDPR and 76.2 of the LOPDGDD, with regard to the infringement of Article 15 of the GDPR, makes it possible to impose a penalty of 1000 EUR (one thousand euros).

VII
Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled *'Termination in penalty* proceedings', provides:

'*1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.*

2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (…)'

In accordance with the above:
Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Declare the termination of procedure PS/00206/2022, in accordance with Article 85 of the Spanish LPACAP.

SECOND: Notify this decision to **BANKINTER, S.A.**

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

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the fourth additional provision of Law 29/1998 of 13 July governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

968-171022

Mar España Martí
Director of the Spanish Data Protection Agency