File No: PS/00003/2021
IMI Reference: A56ID 113249- Case Register 123773

FINAL DECISION ON PENALTY PROCEEDINGS

Of the proceedings conducted by the Spanish Data Protection Agency and on the basis of the following

FACTS

FIRST: On 03 March 2020, via the 'Internal Market Information System' (hereinafter IMI), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), which aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, the Spanish Data Protection Agency (AEPD) received a complaint dated 23 December 2018 from [redacted] (hereinafter the complainant) to the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP). This complaint is transmitted 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 the General Data Protection Regulation or GDPR), taking into account its cross-border nature and that this Agency is competent to act as lead supervisory authority.

The complaint is made against *Michael Page International on the* following grounds:

. The complainant, a Dutch citizen, opened an account in the Dutch version of Michael Page International's web portal, accessible at the URL *"www.michaelpage.nl"*, and in March 2018 sent a Curriculum Vitae (CV) for a job offered by the Dutch branch of the PageGroup group. A few months later, she requested access to her personal data via the email address indicated in the Privacy Policy of the web portal, *"gdpr@pagegroup.eu"*.

. In response to the above-mentioned access request, the responsible entity initially required the complainant to provide two out of three categories of identification documentation (passport, national identity card or driving licence), showing the date of birth; social security or national insurance card and invoice for energy supply or water for less than 3 months. However, following the applicant's protest, which considered the request for documentation to be excessive, Michael Page International corrected and requested only a copy of the identification document on both sides.

. The complainant considers that there is no reason to request this identification information, which was not required to open an account on the web portal, or to submit a CV for the purpose of applying for a job. The complainant considers that authenticated access to the account, which is still active, should be sufficient to understand the exercise of the right of conformity and the identity of the applicant in a system such as that used

by the controller, based on the use of a private account.

The complaint provided a copy of the complainant's correspondence with the controller following the request for access, dated 28 September 2018, which was also accompanied. This correspondence is set out in Facts 4 to 9.

The documentation relating to this complaint was supplemented by voluntary assistance in IMI, sent by Autoreit Persoonsgegevens on 12 May 2020, incorporating the consultation which the Dutch authority made to the establishment of the PageGroup group in the Netherlands (Michael Page International — Nederland Bv), in the Dutch language, on decision-making relating to the means and purposes of the processing of personal data concerning residents of the Member States.

The reply given by that establishment to the abovementioned consultation, in English, states that, although the headquarters of the group are located in the United Kingdom, the department responsible for managing access requests for continental Europe is the Legal Compliance Team, located at the Centre for Shared Services in Barcelona (Spain). The postal address of that department is indicated in the Privacy Policy of the Dutch version of the Responsible Officer's website, accessible in the URL *"https://www.michaelpage.nl/en/privacy"*.

According to that reply, the Spanish establishment of the group of companies would be the main establishment within the meaning of the definition in Article 4 (16) of the GDPR. Thus, in accordance with Article 56 (1) of the GDPR, on 21/05/2020, the AEPD declared itself competent to act as lead supervisory authority (LSA).

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, in addition to the supervisory authority which reported the case (the Netherlands), Belgium, Ireland, Poland, Italy, Hungary, Portugal, Cyprus and Austria, as well as the German regional authorities of North Rhine-Westphalia, Rhineland-Palatinate, Mecklenburg-Western Pomerania, Berlin and Bavaria Private Sector, have declared themselves concerned in the present proceedings.

SECOND: In accordance with the procedure laid down in national legislation (Article 64 (3) of the Spanish Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights — LOPDGDD), on 11 June 2020, the AEPD transmitted the complaint to the Spanish establishment of the PageGroup group based in Hospitalet de Llobregat, namely the company PAGE GROUPEUROPE, S.L. ('PAGE GROUP EUROPE'). in order to demonstrate within one month that it responded to the complainant's request, provide information on the reasons for the incident and set out the measures taken to avoid similar situations.

In response to that request, PAGE GROUP EUROPE provided the following communications with the complainant:

. They explain that they are a company that is part of a business group dedicated to human resources services, namely recruitment. For this reason, they process personal data of a high number of candidates in many countries of the world, with the exercise of rights by candidates being very common. In order to process the relevant requests, in compliance with its duty of confidentiality and secrecy, it has implemented a strict identity

verification process to ensure that candidates' personal data are not transferred to third parties, that they may have obtained the access credentials of persons registered in their systems for the purpose of deleting their identity and making the application on their behalf, through phishing or social engineering attacks.

. In the particular case of the complainant, they have not sought to hinder the exercise of her rights, but rather to protect her personal data. In fact, as is apparent from the communications submitted by the interested party, the opportunity was offered to provide a copy of her ID as an alternative to the initial procedure, which required the production of two documents proving identity, without any reply from the complainant.

. It adds *that "it has abolished the procedure whereby two out of three categories of identification documentation were requested. At present, PAGE only requests an identification document and also offers alternatives to interested parties, such as signing by means of an electronic certificate, face-to-face care in any office of PageGroup or any other means which the person concerned considers appropriate'*.

On this point, it provides a copy of the 'Reply Models' currently used to verify the identity of the parties concerned. The first of these requests the person concerned to copy the identity card or EIN, passport or driving licence with date of birth, any of them; attention is also drawn to the possibility of using alternative means, should the person concerned prefer not to send such documents. The second model refers to such alternative means, such as the presence in a Group office or the sending of a document signed by means of an electronic certificate.

Subsequently, by letter of 14 August 2020, the Agency asked PAGE GROUP EUROPE *'a copy of the reply to the request for access raised by the complainant, since its identity has been proven through the complaint procedure initiated before the supervisory authority of the Netherlands and continued at this Agency'*. Following this request, the aforementioned entity responded to the complainant's request for access and provided the Agency with a copy of the communication dated 27 August 2020 informing the Agency of the aspects of the processing provided for in Article 15 of the GDPR, as well as the annex containing the complainant's personal data in its possession. The reply to this Agency states that the information was sent by e-mail.

THIRD: Having reviewed the reply provided by the company complained of, as set out in the previous facts, the Agency found that, at present, the procedures followed by PAGE GROUP EUROPE for the attention of data protection rights, in relation to the identification of applicants, comply with the applicable legislation. Considering that the documents it manages as a company active in the human resources sector contain a lot of personal information, the requirement to request additional identification documentation in order to comply with a request for access was considered reasonable, taking into account the 'phishing' or social engineering attacks that may occur, as well as unauthorised accesses that suffer from email accounts worldwide.

In addition, it was taken into account that, following the intervention of this Agency, the complainant's request for access was granted.

Consequently, it was considered that there was no evidence of an infringement and that no further action was necessary or that further action was required, so that, on 10

November 2020, a draft decision to discontinue proceedings was issued.

FOURTH: On 10 November 2020, the draft decision was incorporated into the IMI system so that the authorities concerned could make their views known.

At the end of the deadline, the Data Protection Authorities of Portugal (CNPD) and Berlin (The Berlin Commissioner for Data Protection and Freedom of Information -Berlin DPA) raised objections to the above-mentioned draft decision.

The CNPD states that PAGE GROUP EUROPE has implemented a rights clearance procedure whereby it requests identification documentation in any case, without taking into account the circumstances of each request, and has not specified that in the case of the complainant it had doubts regarding her identity. It considers that the aforementioned entity has failed to comply with Article 12 (2) of the GDPR, which obliges the controller to facilitate the exercise of the rights, unless it is unable to identify the applicant, in which case Article 12 (6) of the GDPR allows additional identification information to be requested.

Also understands from the CNPD that the procedure followed by the responsible entity does not protect the data of the applicants, as the processing of the required identification documents increases the risks for those concerned (e.g. possible use for identity theft); it also takes into account that this documentation was not required from the complainant to open an account or send a CV. The Portuguese authority believes that this violates the principle of minimisation (Article 5 (1) (c) GDPR), privacy by default and by design (Article 25 GDPR) and security measures (Article 32 GDPR).

The CNPD advocates a less intrusive way of verifying the identity of the applicant (e.g. electronic identification or sending the request via the user account together with an additional authentication factor submitted via another channel).

Berlin DPA, for its part, also finds an infringement of Article 12 (2), (3) and (6) of the GDPR for reasons similar to those put forward by the Portuguese authority. Considers that additional information should only be requested if there are doubts as to the identity of the data subject, requesting necessary and appropriate information for such verification, on the basis of the applicant's available data; it does not share the justification put forward regarding the possible risk of emails being buried. Furthermore, given that the ID card was not required to register, Berlin DPA considers that it cannot be used for verification purposes, or at least would not be the most appropriate form, and agrees with the complainant's assessment that registered access to the private account would be more than sufficient.

Berlin DPA points to a possible infringement of Article 12 (3) GDPR because the controller did not reply within one month of the submission of the request.

It objects to the rejection of the complaint and considers it appropriate to identify infringements and take corrective measures against the controller so that it can correct its procedures in order to avoid jeopardising the rights of other applicants or the obstacles to their exercise.

FIFTH: The objections raised by the data protection authorities referred to in the previous

Facts have been taken into consideration and, on 11 December 2020, the complaint communicated by the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) was declared admissible, without prejudice to what may be determined in the course of the processing of the complaint.

SIXTH: On 26 February 2021, the General Subdirectorate of Data Inspection accessed the website *'www.michaelpage.es'* and obtained information on PageGroup.

The corporate information in the section *'What are we'* on that website states:

"PageGroup is the leading international consultant in the selection of qualified, middle and senior managers on a temporary and indefinite basis. It was established in the United Kingdom in 1976 and has been listed on the London Stock Exchange since 2001. With a network of 140 own offices, we operate in 36 countries around the world. In Spain, we offer coverage at national level with physical offices in Madrid, Barcelona, Valencia, Seville, Bilbao and Zaragoza through which we provide recruitment services and career opportunities at local, regional and global level. Within the group we have different brands, each expert on its market".

The website *"www.pagegroup.com"* is also accessed and the annual report for 2019 (*"Annual Report 2019"*) is obtained. According to the information contained in this document, which is incorporated into the actions, PageGroup made a gross profit of GBP 855,5 million in 2019 and an operating profit of GBP 146,7 million.

According to the information in the Central Commercial Register concerning PAGE GROUP EUROPE, the 'subscribed capital' amounts to 60 000,00 EUR.

Information on PAGE GROUP EUROPE is available on the website "axexor.es", which shows a sales volume of more than 34 million EUR. The number of employees is 376.

SEVENTH: On 02 June 2021, in accordance with Article 64 (2) (third subparagraph) and (3) of the LOPDGDD, a revised draft decision to initiate penalty proceedings was issued on the basis of the complaint received via the IMI system, as set out in the First Fact. This revised draft decision takes into account the objections set out in the Fourth Fact.

In accordance with the procedure laid down in Article 60 of the GDPR, on 13 March 2020, the aforementioned revised draft decision to initiate penalty proceedings was sent via the IMI system to the supervisory authorities concerned, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate penalty proceedings would be adopted.

None of the supervisory authorities concerned has raised any objection to the revised draft decision to initiate penalty proceedings adopted by the AEPD, and it is therefore understood that there is agreement on it.

EIGHTH: On 29 June 2021**,** the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against PAGE GROUP EUROPE, in accordance with Articles 63 and 64 of the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), for the alleged infringement of Articles 5.1 (c) and 12 of the GDPR, as set out in Articles 83.5 (a) and (b) of the same Regulation, respectively; establishing that the fine that might be applicable would amount to a total of 300,000 EUR (250,000 EUR for the infringement

of Article 5 (1) (c) and 50,000 EUR for the infringement of Article 12, both of the GDPR), without prejudice to the outcome of the proceedings.

The same decision initiating the procedure stated that the alleged infringements, if confirmed, could lead to the imposition of measures, in accordance with the provisions of Article 58 (2) (d) of the GDPR.

NINTH: Having notified the above-mentioned decision to initiate proceedings and extended the deadline for submitting allegations, PAGE GROUP EUROPE submitted a letter dated 21 July 2021, requesting that the AEPD's initial approach be maintained and that the penalty proceedings be closed or, in the alternative, that the proposed fine be reconsidered, taking into account the reprimand provided for in the legislation. In summary, that entity bases its request on the following considerations:

1. As a preliminary point, it highlights the good faith and willingness to comply which has governed its action and the internal policies applied, and expresses its intention to provide more information and clarity with its arguments on the case, despite the fact that it entails a waiver of the application of the reduction of the proposed penalty, in the belief that they have followed the recommendations of the authorities and that their motivation was only an excessive zeal in the protection of personal data for not giving data to a person other than the beneficial owner of the data. It adds that the question raised concerns an interpretation of the provision, which is still only recently applied.

2. It takes the view that it is contradictory to state in the legal bases of the opening agreement that the outcome of the transfer procedure *'was not satisfactory'*, when it is stated in the Second and Third Fact that the requested party responded to the request for access made by the complainant, that the procedures currently applied for the attention of rights comply with the applicable legislation or that the request for additional identification documentation was considered reasonable, concluding that there were no indications of infringement and that it was not necessary to adopt additional measures.

On this basis, it requests that the documents in the file be reviewed again, clarifying in this regard, in the event that the statement is motivated by the absence of a reply to the Dutch authority's first request, that in June 2019, access to dpo@page.com was granted to persons in the Legal Compliance Team on a temporary basis, on the ground that the person providing DPD services would leave the company at the beginning of July 2019 and until another person took up those duties, although for some technical reason the connection was only effective at the end of August, without it being possible to recover the emails received in the meantime.

As soon as it became aware that the Dutch Data Protection Authority (Autoreit Persoonsgegevens -ap) had sent 2 emails on 23 July 2019, it contacted it, although there is no record of having received a reply.

Subsequently, on 30 August 2019 Autoreit Persoonsgegevens sent a letter directly to Michael Page International — Nederland Bv, to which it replied on 27 September 2019.

3. In relation to the alleged infringement of Article 5 (1) (c), it highlights the review of its internal policies carried out in 2016-2018 in order to bring them into line with the new legislation, on which there were no guiding criteria for interpreting novel concepts such

as the principle of data minimisation or privacy by design or by default. It therefore tried to combine measures and recommendations that remained in force with an interpretation of the new legislation aimed at strict compliance with it.

This process included reviewing and updating the procedure for dealing with the rights of those affected, with three key measures, such as the appointment of a DPO and the centralisation of that procedure in PAGE GROUP EUROPE, which was granted the power to decide whether the request for the exercise of rights was valid or required an application for an identification document in order to verify the identity of the person concerned and to process the exercise of rights.

According to the internal criteria followed, no identity document was requested in the exercise of rights relating to requests for rectification, erasure or forgotten, limitation or objection, but in cases where the exercise of the right of access or portability was requested, which involve the provision of curriculum vitae data that may contain relevant information. It was intended to confirm identity in order to protect those affected from possible identity theft and it was understood that the possession of an official document matching the name and surname with the information available in the database was a credible evidence that the same person was involved.

It then pointed out that few requests had been received since May 2018 and provided details of the access requests processed since that date:
. 2018: 50 requests for access, representing 1.66 % of the total
. 2019: 62 requests for access, representing 1.56 % of the total
. 2020: 55 requests for access, representing 1.65 % of the total
. 2021: 28 requests for access, representing 1.63 % of the total

On the other hand, as regards Berlin DPA's interpretation of the appropriate means of verifying the identity of the data subjects exercising a right, the requested body considers that those assessments derive from local idiosyncracy and may be motivated by historical issues, inherited from previous local regulations, cultural or compliance aspects, which will be defined and standardised over the coming years.

After analysing the German Identity Document Act ('Personalausweisgesetz'), it requests that the facts and conclusions be reviewed in the light of the following circumstances:

— The presentation of a copy of the identity card was deemed necessary only in the requests for the exercise of the right of access and portability as there was an increased risk of sharing data with a person other than the beneficial owner of the data because of the reasonable doubts about the identity of the person arising from phishing and forging of usual practices and a real concern in the recruitment sector; Page has suffered several attempts of cyber fraud by third parties to pass through their employees in an attempt to obtain personal data from data subjects. Due to distance, it is not only possible to display the identity card by the person concerned at the company's registered office or at a branch, and it was therefore considered necessary to request a digital copy of the identity card for this purpose;
— Only the legal compliance team had access to such a document, which it used only to verify identity, not including the document on the file of the person concerned or carrying out any further processing;

— Only the first name and surname were checked for identification purposes. The other data, according to that German law, could and should have been crossed out by the data subject at the time of shipment (for example, access and serial numbers, nationality, date of birth, stature, colour of eyes, photograph and machine-readable zone). The German legislation already provides for other information to be obscured. We therefore consider that it is common practice in Germany to request this type of documentation for verification purposes.
Furthermore, the requested entity claims to have studied that the Dutch authority has been active as regards the illegal processing of the BSN (Personal Identification Number) and has taken several enforcement measures before the entry into force of the GDPR, including:
. Airbnb unlawfully dealt with the BSN (through complete copies of the identity documents) and the DPA published its findings in this regard. No fine was imposed and no investigation report was published after Airbnb changed its operations.
. A freight company called Nippon Express processed complete copies of the identity documents and BSN of the lorry drivers entering the premises to collect the cargo. This was illegal according to the Dutch DPA and published an investigation report without penalising the company after changing its procedures.

As can be seen, and will be further developed, the requested entity does not derive any benefit from extending or allegedly hindering the exercise of a right which entails the provision of information to the data subject. This is not a departure from a service or an objection to a particular treatment that the entity had an interest in maintaining.

That measure was understood to be proportionate by assessing, on the one hand, the damage that could be caused by providing curriculum vitae information to third parties other than the holder with regard to the 'inconvenience' which may involve sending/displaying an identity document, which most citizens are already scanned.

On the basis of this, it requests that the arguments of Berlin DPA and the CNPD that changed the AEPD approach, which decided to close the procedure as it did not assess intent in the action carried out by PAGE GROUP EUROPE, be reconsidered because of the lack of profit and the improvement implemented.

4. The processing carried out, consisting of verifying the match of the first name and surname of the document with those in the database, complies with the principle of minimisation (recital 39 GDPR): the requested document was suitable to allow for such verification; it is relevant because it does not involve a disproportionate effort on the part of the operator to submit it; the processing of that document was limited to what was necessary in relation to the purposes for which it was processed, without adding any additional information contained therein to the data subject's file and without any further processing of the document. Similarly, the concept of restriction of access was incorporated, since that data was processed only by the Legal Compliance Team, which did not process that document subsequently. It therefore does not represent an additional risk for the data subject.

Considering this lack of further processing and the fact that the processing carried out was very limited in time, as was the access to the information in question, the requested entity considers that recital 156 of the GDPR is complied with: *'The conditions and safeguards in question may include specific procedures for the exercise of those rights*

by data subjects if it is appropriate in light of the purposes for which the specific processing is carried out, together with technical and organisational measures aimed at minimising the processing of personal data having regard to the principles of proportionality and necessity'; it was considered, after consideration, that this measure was necessary, proportionate and appropriate to protect the rights of the person concerned.

5. With the aforementioned requirement, the respondent did not attempt to extend, hinder or hinder the exercise of rights by the person concerned, nor did it benefit from that practice, which required a specific procedure to be designed and resources invested in management and monitoring. If, finally, it is established that such a procedure was not properly designed, the only thing that can be attributed to it is an excess of the intention to comply with it, in order to ensure that no data was handed over to a person other than its holder, but not that this request was intended to hinder the exercise.

The entity considered as likely a scenario of identity theft, in which one person would access the email or account access keys of another person, in order to obtain the data from that account, and therefore considered an alternative means other than the usual authentication of the user.

6. With regard to the alleged infringement of Article 12 of the GDPR, the respondent puts forward arguments seeking to respond to the arguments put forward by the data protection authorities of Berlin and Portugal, but do not start by insisting that the entity is alert to access requests because they are not frequent in its activity, since it is the data subjects themselves who directly provide their personal data and have the information available to them in their personal area.

With regard to Berlin DPA's statement, which does not share the potential risk of emailing e-mail addresses, the respondent shows that there are studies and statistics that demonstrate the hypothesis that the request for the right of access to the GDPR may be a point of vulnerability to social engineering attacks.

And adds:

"To cite some of these studies, James Pavur (DPhil researcher Oxford University) and Casey Knerr (Security Consultant Dionach LTD) state in their publication "GDPArrrrr: Using Privacy Laws to steal Identities':
"In this work, we have raised the hypothesis that the right to request access can be a point of vulnerability to social engineering attacks. Through an experiment covering 150 organisations, we demonstrated the feasibility in the real world of such attacks. We found that a large proportion of organisations do not adequately verify the origin identity of access requests and that, as a result, deeply sensitive information can be acquired repeatedly and scalable by social engineering. We suggest a number of corrective measures focused on individuals, businesses and legislators to help mitigate these attacks.
(...)
Requesting a photo identification issued by the government is probably the most robust way to prevent this attack. However, organisations that are not able to adequately protect this data, or to verify its authenticity, should consider subcontracting these services to a third party.
Companies should also regularly assess their process of requesting access from the subject in search of vulnerabilities and train individual representatives of the service in detecting and responding to such attacks. The addition of malicious access requests...".

Recital 64 GDPR itself states that *'The controller should use all reasonable measures to verify the identity of a data subject who requests access'*. Furthermore, Article 12 (6) GDPR provides *that 'where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject'.*

In Spain, the need to provide the identity card or equivalent document by the data subject was provided for in Article 25 of the repealed, almost entirely, Royal Decree 1720/2007. That article stated that notification of the exercise of rights to the controller should be accompanied by a photocopy of the person's national identity card, passport or other valid document identifying him.

The Spanish Data Protection Agency itself (AEPD), in its *'Guide for the Citizen'*, states that *'if the controller has doubts as to the identity of the data subject, it may request additional information in order to confirm it, such as a photocopy of the ID card, passport or other valid document'*.

In addition, the forms that the AEPD designed as models for the exercise of rights and which it presents as templates for use by citizens include the following instruction:
'2. A photocopy of the D.N.I. or equivalent document proving identity must be provided and considered valid in law, in cases where the person responsible has doubts as to his identity. In the event of legal representation, the identity card and document certifying the representative's representation must also be provided'.

This is therefore a common practice, at least in Spain, the residence of our company, which does not violate the principle of data minimisation, which requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Claims that it made an error in explaining the duty clearance procedure implemented, which led to the CNPD's indication of the request for *'identification documentation in any event, without taking into account the circumstances of each application, and did not specify that in the case of the complainant it had doubts regarding its identity'*; it points out that this internal procedure (attached as an annex) specifies that the identity of the applicant is checked in case of reasonable doubts about it ('Request valid'), in which case it is verified by requesting an ID validation.

This measure was taken in compliance with the principles of data protection by design and by default, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity of the processing for the rights and freedoms of natural persons, taking into account the amount of personal data collected (identification card), the extent of their processing (verification of consistency with the data of the data subject available), their storage period (erased immediately after verification) and their accessibility (only the Legal Compliance Team, and ultimately the DPO had access).

With regard to the increased risks for those affected, also highlighted by CNPD, it reiterates once again that the identity document was required only in the exercise of the right of access, not in other rights, and that all the necessary technical and organisational

measures were put in place so that, once the check had been carried out, the document received was deleted.

7. Stresses once again the good faith and degree of collaboration shown, having modified the internal rights management procedure as follows:

The Legal Compliance Team validates the identity of the applicant, which is considered validated if the first name, surname and e-mail match those in the database. Additional information is requested only when we have reasonable doubts about the identity of the applicant.

The criteria for determining whether there are doubts about the identity of an applicant are:
I. Receiving the access request from a valid email address recorded in the database is sufficient to verify the identity of the applicant.
An email response is sent to the requester confirming receipt of his/her right of access.
II. If there are reasonable doubts about the identity of an applicant, for example because there are several persons with the same name, or there are duplications/doubts about the e-mail address, additional information is requested to verify his/her identity by email, explaining to the applicant the existence of doubts about his/her identity and the need to confirm it. Only information that is already in the applicant's profile, e.g. postcode or the last 3 digits of the applicant's telephone number, is requested.

8. It refers to the closure of the proceedings initially adopted by the AEPD and to the objections of the Portuguese (CNPD) and German (Berlin DPA) authorities, in order to highlight the uncertainty caused by the lack of unity of the criterion for verifying online identity during the management of a right of access.

The GDPR does not lay down, as was the case under the previous legislation, the list of security measures that controllers must adopt; each controller must now carry out its own risk analysis and determine what measures it should take to mitigate them, and this was acknowledged by the AEPD, which considered it reasonable in this case to request additional identification documentation, taking into account the information available, the 'phishing' or social engineering attacks that may occur and unauthorised access to e-mail accounts worldwide.

This is an interpretation based on risk analysis and from good faith and belief of good action, applying the principles of minimisation, privacy by design and by default, on a specific subject (request for identification in the right of access) on which there is no published criterion or guide.

9. With regard to the criteria for graduating the penalty, it states the following:

. Negligence in committing the infringement must be assessed when the conduct deviates from recognised standards and, in this case, when applying for an identity document while managing a right of access, it can now be regarded as 'standard'. In addition, the proactive and improved attitude should be taken into account.

. The volume of data and processing covered by the file is limited to the claim of a single person, or in general annual numbers an average of 55 persons per year, of whom only

one person has requested in the last 4 years.

. The assessment of the number of data subjects should consider the rights exercise requests received since the GDPR is fully implemented, already detailed.

. This is the first time that the requested entity has been the subject of penalty proceedings, complying so far with the obligations laid down in the applicable legislation and with the criteria laid down by the supervisory authorities.

In that regard, it requests that consideration be given to the imposition of a reprimand with particular regard to the nature, minor gravity and short duration of the infringement, its unintentional nature, the measures taken to remedy the damage suffered and the degree of liability demonstrated by the entity.

Page GROUP EUROPE, with its written observations on the opening of the proceedings, submitted the following documents:

. Copy of the document called *"EU GDPR Data Request Process"*. The provisions it contains on the validation of applications for rights and verification of the identity of applicants are set out in Fact 12.
. Post registration received in the meantime of the technical failure in email from the DPO.
. Letter of 26 August 2019, sent to the Dutch authority requesting the sending of the missing communication.
. Letter with the documentation sent in September 2019 to the Dutch Data Protection Authority.

TENTH: On 24 November 2021, a motion for a resolution was issued as follows:

1. That the Director of the AEPD penalises PAGE GROUP EUROPE for an infringement of Article 12 of the GDPR, defined in Article 83 (5) (b) of the GDPR and described as minor for the purposes of limitation in Article 74 (c) of the LOPDGDD, with a fine of 50,000 EUR (fifty thousand euros).

2. That the Director of the AEPD penalises PAGE GROUP EUROPE for an infringement of Article 5 (1) (c) of the GDPR, defined in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (a) of the LOPDGDD, with a fine of 250,000 EUR (two hundred and fifty thousand euros).

The aforementioned draft decision was notified to PAGE GROUP EUROPE on the same date as 24 November 2021. This notification informed this entity that, in accordance with the provisions of Article 85 (2) of the LPACAP, it may, at any time prior to the resolution of the procedure, make the voluntary payment of the proposed penalty, which would result in a reduction of 20 % of the amount of the penalty. With the application of this reduction, the penalty would be set at 240,000 EUR (two hundred and forty thousand euros) and its payment would lead to the closure of the procedure. It was also noted that the effectiveness of this reduction is conditional on the withdrawal or waiver of any administrative action or appeal against the penalty.

ELEVENTH**:** On 02 December 2021, the requested party paid the penalty in the amount

of 240,000 EUR, making use of the reduction provided for in Article 85 of the LPACAP, which means that the procedure is terminated and any administrative action or appeal against the penalty is waived.

TWELFTH: On 03 December 2021, we received a letter from PAGE GROUP EUROPE dated 02 December 2021, submitting a copy of the proof of the payment made, which it intended *to 'close'* the procedure. In the same letter, the aforementioned entity draws attention to the confidentiality of corporate internal processes.

The actions taken in these proceedings and the documentation contained in the file have shown the following:

PROVEN FACTS

1. Michael Page International is a UK-based company, the parent company of the PageGroup group. It is dedicated to staff selection and operates under various brands, including *'Michael Page'*. It has subsidiaries in many European countries, the subsidiary of the Netherlands being Michael Page International — Nederland B.V.

One of the Group's Spanish subsidiaries, based in Hospitalet de Llobregat, PAGE GROUP EUROPE, S.L., is responsible, through its Legal Compliance Department, for managing requests for the exercise of personal data protection rights that data subjects make to the entities of the PageGroup Group in Europe. The postal address of this Spanish subsidiary is indicated as the contact details for the exercise of these rights in the entity's privacy policy, both in Spain and in the Dutch version.

2. PageGroup's websites include a form that allows data subjects to send their CVs to the relevant subsidiary entity.

3. The complainant, a Dutch citizen, opened an account on the website of Michael Page International — Nederland B.V., accessible at the URL *"www.michaelpage.nl"*, and sent a Curriculum Vitae (CV) for a job offered by this Dutch subsidiary of the PageGroup group in March 2018.

4. By email dated 28 September 2018, sent from the address [redacted], the same as recorded in the PageGroup database, the complainant requested access to her personal data, expressly specifying in her request that a copy of her data be sent to her and her interest in knowing the purposes for which the data are processed, the categories of personal data processed, the recipients and the legal basis for each processing operation. That email was sent to the address *'gdpr@pagegroup.eu'*, which corresponds to that indicated for that purpose in the Privacy Policy accessible through the web portal.

In this email, the complainant warns that she receives regular emails from the entity and that this proves that her personal data is available to her.

5. By email dated 02 October 2018, sent from the address *'gdpr@pagegroup.eu',*

PageGroup replied to the complainant's email of 28 September 2018, stating that in order to comply with the request for access it was necessary to confirm her identity and prove her address. To this end, the complainant is requested to provide two out of three categories of identification documents: (I) passport, national identity card or driving licence showing date of birth; (II) social security or national insurance card; (III) invoice for public services aged less than 3 months. It is also stated that this documentation can be sent to *"gdpr@pagegroup.eu"* or to the Legal Compliance Department by post to PAGE GROUP EUROPE in Hospitalet de Llobregat.

In addition, this reply informs that if the personal data do not match the recorded ones, further documents will have to be requested and that once the identity has been validated, a copy of the information will be provided within one month.

6. By email dated 20 October 2018, sent to the address *"gdpr@pagegroup.eu"*, the complainant notes that it does not have public utility invoices and that the identification by means of the identity and insurance documents it requires constitutes excessive data processing or an impediment to the exercise of her right. She also points out that the identification process is simplified by considering that she has an account on the entity's website.

7. On 22 October 2018, the Legal Compliance Department of PageGroup sent an email to the complainant, from the address *'gdpr@pagegroup.eu'*, reiterating the need to verify her identity and insisting on the request for earlier documentation.

8. On 11 November 2018, by email sent to the address *'gdpr@pagegroup.eu'*, the complainant, after summarising the facts and highlighting her interest in knowing the communications of personal data made to third parties and the specific data shared, reiterated her previous statements on the documentation required to comply with that request, which she considered excessive, and warned about the possibility of lodging a complaint with the Dutch data protection authority.

9. On 12 November 2018, the PageGroup Legal Compliance Department sent an email to the complainant, from the address *'gdpr@pagegroup.eu'*, informing that they had reviewed her request and requesting that a copy of her identity document be sent by both parties in order to proceed with the request for access.

10.By letter of 14 August 2020, this Agency asked PAGE GROUP EUROPE *'a copy of the reply to the request for access raised by the complainant, since her identity has been proven through the complaint procedure initiated with the supervisory authority of the Netherlands and continued at this Agency'*. Following that request, the aforementioned entity responded to the complainant's request for access and provided the Agency with a copy of the communication dated 27 August 2020, replying to the complainant's request for access, as well as the annex containing the personal data held by PageGroup. The reply to this Agency states that the information was sent by e-mail.

11. In its letter of 10 July 2020, lodged on the same date with the AEPD, PAGE GROUP EUROPE stated that it *'has abolished the procedure whereby two out of three categories of identification documentation were requested. At present, PAGE only requests an identification document and also offers alternatives to data subjects, such as signing by means of an electronic certificate, face-to-face care in any office of PageGroup or any*

other means which the person concerned considers appropriate'.

With that letter, it produced a copy of the new 'Reply Models' used to verify the identity of the data subjects. The first of these requests the person concerned to copy the identity card or EIN, passport or driving licence with date of birth, any of them; attention is also drawn to the possibility of using alternative means, should the data subject prefer not to send such documents. The second model refers to such alternative means, such as the presence in a Group office or the sending of a document signed by means of an electronic certificate.

12. PAGE GROUP EUROPE, with its written observations on the opening of the procedure, has provided a copy of the document entitled *'EU GDPR Data Request Process'.*

This document indicates that requests to exercise rights are validated if the first name, surname and e-mail match those recorded in their database. In the case of requests for access and portability, it is added that additional information should be requested when there are reasonable doubts about the identity of the applicant, and clarifies that this is the case where there are several persons with the same name or in case of duplication/doubt about the email address.

For the request for additional information, it is envisaged to send an email requesting information already contained in the applicant's profile registered in his database, and citing as an example the postcode or the last three digits of his or her telephone number.

A template of this request for information is included, requiring one of the two data elements indicated above (postal code and three last digits of the telephone number) and warning that if the data subject does not wish to provide such information, he/she may alternatively apply to a PageGroup office or send a digitally signed document; or communicate whether it has a different means.

In the event that, for any reason, they could receive an identity card or similar documentation from any person concerned, the immediate deletion of that information is required, without using it for validation purposes.

As regards the submission of the document by which the right of access is respected and the corresponding information is provided to the person concerned, the procedure designed by the requested entity provides for it to be sent by email, protected by a password which is sent in a different post.

LEGAL GROUNDS

I

By virtue of the powers conferred on each supervisory authority by Article 58 (2) of the GDPR, and in accordance with Articles 47, 64.2 and 68.1 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to initiate this procedure.

Article 63.2 of the 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'.

Paragraphs (1) and (2) of Article 58 GDPR list, respectively, the investigatory and corrective powers that the supervisory authority may have for that purpose, by mentioning in point 1 (d) the *power to 'notify the controller or processor of an alleged infringement of this Regulation*'; and in paragraph 2. (i), '*to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case'*.

The case under consideration is based on a cross-border complaint to the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) against a group of companies based in the United Kingdom. However, the department responsible for managing access requests for continental Europe is the Legal Compliance Team of the subsidiary of the PAGE GROUP EUROPE Group, based in Spain. This Spanish establishment of PageGroup is the Group's main establishment, within the meaning of the definition in Article 4 (16) GDPR. Thus, in accordance with Article 56 (1) GDPR, the AEPD is competent to act as lead supervisory authority.

The following *'definitions'* set out in Article 4 GDPR are taken into account:

'(16) main establishment:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.'

"(21) supervisory authority: the independent public authority which is established by a Member State pursuant to Article 51."

"(22) supervisory authority concerned: the supervisory authority which is concerned by the processing of personal data because:
A.- The controller or processor is established on the territory of the Member State of that supervisory authority;
B.- Data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing, or
C.- A complaint has been lodged with that supervisory authority.'

"(23) cross-border processing:
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State;
or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, the personal data protection authorities of the Netherlands, Belgium, Ireland, Poland, Italy, Hungary, Portugal, Cyprus and Austria, as well as the German

regions of North Rhine-Westphalia, Rhineland-Palatinate, Mecklenburg-Western Pomerania, Berlin and Bavaria Private Sector, are acting as *'concerned supervisory authorities*' in the present proceedings.

II

Article 56 (1) of the GDPR, *on 'Competence of the lead supervisory authority*', provides:

'1. Without prejudice to Article 55, the supervisory authority of the main establishment or of 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 set out in Article 60'.

Article 60 governs 'Cooperation between the lead supervisory authority and the other supervisory authorities concerned':

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.
(…)
12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.'

With regard to the matters governed by these provisions, account is taken of recitals 124, 125, 126 and 130 of the GDPR, in particular the following:

(124) '... that authority (the lead authority) should cooperate with the other authorities concerned...'.
(125) 'as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process'.
(126) 'the decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned...'.
(130) 'Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority'.

In accordance with Article 4 (24) GDPR*, 'relevant and reasoned objection*' means the following:

'an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union'

In accordance with the above rules, in the present case, concerning a complaint lodged with the supervisory authority of a Member State (the Netherlands), in relation to processing operations in the context of the activities of an establishment of a controller which affect or are likely to substantially affect data subjects in more than one Member State (cross-border data processing), the lead supervisory authority, in this case the Spanish Data Protection Agency, is required to cooperate with the other authorities concerned.

The Spanish Data Protection Agency, in application of the powers conferred on it by the GDPR, is competent to adopt decisions designed to produce legal effects, whether the imposition of measures ensuring compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their views into account to the greatest extent. It also provides that the binding decision to be taken is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority shall, without delay, forward to the other supervisory authorities concerned a draft decision for their opinion and shall take due account of their views, in accordance with the procedure laid down in paragraphs 4 et seq. The supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no authority objects within the period indicated, in which case all of them are bound by the draft decision.

In another case, i.e. if any of the authorities concerned raises a relevant and reasoned

objection to the draft decision, the lead supervisory authority may follow the objection by submitting to the opinion of the other supervisory authorities concerned a revised draft decision, which shall be submitted to the procedure referred to in paragraph 4 within two weeks. If no further action is taken in the objection or if the objection is deemed not to be relevant, the lead supervisory authority should refer the matter to the consistency mechanism provided for in Article 63 GDPR.

In the present case, the AEPD initially considered that there was no indication of an infringement and that it was not necessary to call for the adoption of measures additional to those implemented by PAGE GROUP EUROPE, with the result that, on 10 November 2020, a draft decision was issued, whereby the other supervisory authorities concerned were required to close the complaint (Draft Decision).

At the end of the prescribed period, the Data Protection Authorities of Portugal (CNPD) and Berlin (The Berlin Commissioner for Data Protection and Freedom of Information — Berlin DPA) raised objections to the draft decision, as set out in the background to this agreement.

Taking into account the reasons set out in the objections raised, and in accordance with Article 60(1) of the GDPR, as transcribed above, which obliges the lead supervisory authority to cooperate with the other authorities, in an effort to reach consensus, the procedure provided for in Article 60 (5) was followed instead of resorting to the consistency mechanism provided for in Article 63 of the GDPR.

Although, as the requested entity points out in its submissions, it initially considered that there were no indications of an infringement, after analysing the observations or objections raised by the supervisory authorities concerned, certain circumstances were revealed which had not been sufficiently assessed in the draft decision, which will be set out in the following legal grounds.

It was therefore appropriate to draw up a revised draft decision providing for the opening of penalty proceedings against PAGE GROUP EUROPE.

This is in line with the cooperation procedure regulated in Article 60 GDPR; it also takes into account Article 58 (4) of the same Regulation, according to which the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

Spanish procedural rules, in particular Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), provide that proceedings of a sanctioning nature shall always be initiated ex officio by agreement of the competent body, which must contain, among other information, the identification of the person or persons presumed to be responsible, the facts giving rise to the initiation of the proceedings, their possible classification and the penalties that may apply.

The adoption of the draft agreement initiating penalty proceedings is provided for in Article 64 (2) (third subparagraph) and (3) of the LOPDGDD, with the obligation to give formal notice to the person concerned. That notification interrupts the limitation period for the infringement.

The revised draft decision drawn up by the AEPD, in the form of a draft initiating penalty proceedings, was submitted for consideration to the authorities concerned, so that they could raise any objections they considered relevant or agree to them. To that end, it was sent via the IMI system to those authorities, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate penalty proceedings would be adopted. None of the supervisory authorities concerned raised any objections and it was therefore understood that there was agreement on the draft in question.

Consequently, on 29 June 2021, the AEPD decided to initiate the present penalty proceedings, in accordance with the arguments and allegations contained in the draft revised decision.

Furthermore, Article 64 (4) of the LOPDGDD provides that the processing times laid down in this Article are automatically suspended when information, consultation, request for assistance or mandatory ruling from a body, office or agency of the European Union or from one or more supervisory authorities of the Member States must be obtained in accordance with the GDPR, for the time between the request and the notification of the decision to the Spanish Data Protection Agency.

III

In accordance with Article 55 of the GDPR, the Spanish Data Protection Agency is responsible for carrying out the tasks assigned to it in Article 57 of the GDPR, including enforcing the Regulation and raising awareness among controllers and processors of their obligations, as well as dealing with complaints lodged by a data subject and investigating the reasons for such complaints.

Correspondingly, Article 31 GDPR establishes an obligation for controllers and processors to cooperate with the supervisory authority upon request in the performance of their tasks. In the event that they have appointed a data protection officer, Article 39 of the GDPR entrusts the latter with the task of cooperating with that authority.

Similarly, Article 65 (4) of the LOPDGDD provides for a mechanism prior to the admissibility of complaints lodged with the Spanish Data Protection Agency, which consists of sending them to the data protection officers designated by the controllers or processors for the purposes laid down in Article 37 of that law, or to the latter where they have not been designated, so that they can analyse those complaints and respond to them within one month.

In accordance with these rules, prior to the admissibility of the complaint giving rise to the present proceedings, it was sent to the responsible entity for analysis, a reply to this Agency within one month and proof that it had provided the complainant with the appropriate reply in the event of the exercise of the rights provided for in Articles 15 to 22 of the GDPR.

The result of that transfer was not satisfactory, given the procedure followed by the draft decision and the objections raised in that regard, so that it was considered appropriate to continue to take steps to clarify the possible responsibilities identified. Consequently,

on 11 December 2020, for the purposes laid down in Article 64 (2) of the LOPDGDD, the Spanish Data Protection Agency declared admissible the complaint communicated by the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) concerning alleged infringements related to the exercise of the rights granted to the holders of personal data. That decision to grant leave to proceed led to the opening of these penalty proceedings.

As regards exclusively a complaint for failure to comply with a request to exercise the rights set out in Articles 15 to 22 of the GDPR, the procedure laid down in Article 64 (1) of the LOPDGDD is followed, according to which:

'When the procedure is exclusively referred to the lack of response to a request to exercise the rights established in articles 15 to 22 of Regulation (EU) 2016/679, it shall be initiated by a resolution to admit for processing, which shall be adopted in accordance with the provisions of Article 65 of this organic law'.

Conversely, where the procedure does not relate exclusively to a request for the exercise of rights, it is necessary to define administrative responsibilities in the context of penalty proceedings, and it is the exclusive competence of the Agency to assess whether there are administrative responsibilities which must be determined in such a procedure and, consequently, to decide on the initiation of such proceedings.

In this case, there are elements justifying the exercise of the sanctioning activity, considering that the procedure provided for in Article 64 (1) of the aforementioned LOPDGDD would not adequately restore the guarantees and rights of the persons concerned.

The origin of the proceedings is determined by a complaint lodged by a specific data subject, which concerns the lack of attention to the right of access exercised by the complainant before the requested body. It could therefore be thought that this is the procedure governed by Article 64 (1) of the LOPDGDD.

However, this claim by an individual has revealed a general action by the controller, and this particular case reflects a common pattern or policy applied to all those affected who are in the same case as the complainant. Where an action which is deemed to be incorrect results from a general policy adopted by the controller, so that it is not a one-off error in a case, the infringement does not lie exclusively in the case under examination but in that general action taken by the controller.

The contrary would be inconsistent with the aim and intention of the Community legislature, which is expressly stated in the GDPR when it states that it is for the supervisory authorities to enforce the rule.

Consequently, this procedure analyses the impact of the general action taken by PAGE GROUP EUROPE on the management and resolution of requests for the exercise of access and portability rights made to it by data subjects, the processing of which is limited and conditional on the documentation requirements generally imposed by that body in order to verify the identity of the applicant, which do not comply with the legislation governing these rights of data subjects, as will be explained below.

In view of the shortcomings noted in the procedure devised by the requested body with

regard to the data protection rules, it appears that those deficiencies are of general application, so that all the data subjects who made the abovementioned requests, and not only the complainant, are affected.

This is concluded in the light of the information and statements that the requested entity itself has provided to this Agency, in which it acknowledges that the process of taking care of rights was in line with the design carried out by the Agency and sets out the reasons that led it to implement a strict identity verification process, based, among other things, on the nature of the human resources services it provides, the large number of candidates and the fact that the exercise of rights is very common, as well as attacks by phishing or social engineering. It defends its system on the ground that it is due to an excessive dirt on the part of the entity.

It expressly stated that it *'abolished the procedure whereby two out of three categories of identification documentation were requested'.*

The information provided by the requested entity is also consistent with the action taken in relation to the complainant's specific request for access.

We therefore do not understand that PAGE GROUP EUROPE, in its submissions to the opening of the procedure, claims that it made an error in explaining the aforementioned rights management process and that it modified its previous approach in order to set out circumstances that do not reflect reality. The fact is that, as demonstrated in the proceedings, the identity verification scheme designed by the respondent applied to all cases of exercise of rights of access and portability, in general, and not only to cases where there were doubts as to the identity of the applicant, as stated in its submissions; that verification required the production by the data subject of several identification documents and not a single document, as appears to be conveyed in the repeated submissions.

Moreover, PAGE GROUP EUROPE states in its written pleadings that it has followed the recommendations of the authorities, however, it does not mention which recommendations would justify the following procedure.

Throughout the text of its written pleadings it refers only to the *"Guide for Citizens"* drawn up by the AEPD and the instructions containing the forms for exercising the rights that the AEPD makes available to citizens via its website. In both cases, as the requested entity rightly points out, citizens are informed of the possibility that the controllers may request photocopy of the ID card or equivalent document, but it should be noted that this should be the case where the controller has doubts about the identity of the applicant and also that the electronic signature may be used instead of the identification document.

The content of those documents does not contradict the criteria set out in this act. It should be noted that the specific objective covered by these guides is to provide guidance on best practices in more general cases, so that they do not cover all specific scenarios that may arise and this implies that the guidance contained therein should be supplemented as appropriate.

Finally, it should be pointed out at this stage that the conclusions set out below are obtained by applying the rules laid down by the GDPR and the LOPDGDD, without

considering repealed legislation, such as Royal Decree 1720/2007, or cultural aspects or historical issues inherited from local regulations, to which the requested entity refers in its written pleadings.

IV

The rights of individuals with regard to the protection of personal data are regulated in Articles 15-22 GDPR and 13-18 LOPDGDD. It provides for the rights of access, rectification, erasure, objection, right to restriction of processing and right to portability.

The formal aspects of the exercise of these rights are set out in Articles 12 GDPR and 12 LOPDGDD.

Article *12 'transparent information, communication and modalities for the exercise of the rights of the data subject*' of the GDPR provides:

'1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(b) refuse to act on the request.
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.
7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly

legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.'

Article 12 (2) and (*4) of the LOPDGDD, 'General provisions on the exercise of rights*', adds the following:

'2. The controller shall be obliged to inform the data subject about the means available to exercise their rights. Such means shall be easily accessible by the data subject. The exercise of the right may not be denied on the sole ground that the data subject chooses a different means'.
'4. The evidence of compliance with the duty to respond to the request for the exercise of rights submitted by the data subject shall be the responsibility of the controller'.

Account is also taken of recitals 59 et seq. of the GDPR.

In accordance with these rules, the controller must devise formulas and mechanisms to facilitate the exercise by the data subject of his or her rights, which shall be free of charge (without prejudice to Articles 12.5 and 15.3 GDPR); is obliged to respond to requests made within one month at the latest, unless it can prove that it is not in a position to identify the data subject; and to state its reasons in case of failure to comply with the request.

It follows from the foregoing that the request for the exercise of rights made by the data subject must in any event be answered, the controller being required to prove compliance with that duty.

This obligation to act does not apply where the controller can demonstrate that it is not in a position to identify the data subject (in the cases referred to in Article 11 (2) GDPR). In cases other than that provided for in this Article, where the controller has reasonable doubts as to the identity of the applicant, the controller may request additional information necessary to confirm that identity.

In that regard, recital 64 of the GDPR is worded as follows:

'(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests'.

As regards the right of access, the GDPR stipulates in its Article 15 that:

"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 recipients to whom the personal data have been or will be disclosed, in particular recipients in third parties or international organisations;
(D) where possible, the envisaged period of storage of personal data or, if that is 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 have not been obtained from the data subject, any available information as to their origin;
(h) the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4), and, at least in such cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject."

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

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'.

Like the other rights of the data subject, the right of access is an extremely personal right. It allows citizens to obtain information about the processing of their personal data, the possibility to obtain a copy of their personal data which are being processed, as well as the information listed in the aforementioned article.

In the present case, the complainant, a Dutch citizen, opened an account in the Dutch version of the website of Michael Page International, accessible at the URL 'www.michaelpage.nl', and sent a Curriculum Vitae (CV) for a job offered by the Dutch subsidiary of the PageGroup group by that channel in March 2018.

Subsequently, on 28 September 2018, she exercised the right of access to her personal data by email sent to the address *'gdpr@pagegroup.eu'*, which corresponds to that indicated for that purpose in the privacy policy of the web portal, expressly stating in this request her interest in knowing the data processed, the purposes for which they are processed, the recipients and the shared data, as well as the legal basis for each processing operation (this request is in line with the content of the right of access provided for in Article 15 of the GDPR), that, as explained above, not only does it involve informing the applicant of the personal data or categories of data processed, so that the exceptional nature attributed to it by the requested entity is not understood when it claims that such requests for access are not frequent since it is the data subjects themselves who directly provide their personal data and have the information available to them in their personal area).

The request made by the complainant is sent from the same e-mail address of the complainant as registered in the PageGroup database, which, according to the complainant, was being used by the Dutch subsidiary of the Group to send her work offers and commercial communications.

In response to this request, on two occasions, the requested entity sent an email to the complainant requiring her to provide documentation proving her identity, establishing this requirement as a condition for complying with the right exercised. In particular, it required the production of two out of three categories of identification documents: (I) passport, national identity card or driving licence showing date of birth; (II) social security or national insurance card; (III) invoice for public services aged less than 3 months.

Also on two occasions, by e-mails dated 20 October and 11 November 2018, the complainant warned that the required identification constitutes excessive data processing or an impediment to the exercise of her right and expressly pointed out that the identification process is simplified by considering that she has an account on the entity's website.

It would not be until 12 November 2018, after the complainant communicated her intention to lodge a complaint with the Dutch data protection authority, when PAGE GROUP EUROPE amended its initial requirements, but maintained the request for the complainant's identity card (copy by both sides) in order to proceed with the request for access.

On the question of verification of the identity of applicants for rights, the rules set out above are clear by stating that this verification process must be limited to specific cases

in which the controller has *'reasonable'* doubts as to the identity of the natural person making the application.

Article 12 (6) GDPR refers to all requests for rights and allows for the possibility to require, in such cases*, "additional information*" necessary to confirm the identity of the data subject. In particular, with regard to access requests in the context of online services, Recital 64 of the same Regulation refers to the possibility for the controller to use all *'reasonable measures'* to verify the identity of data subjects.

The rules governing the exercise of rights do not, therefore, establish the need to provide any specific identification document in order for them to be met, nor do they even require such identity verification to be carried out on the basis of documentation. They refer to the possibility of obtaining *'additional information'* and the use of *'reasonable measures',* whereby it is for the controller to determine what information and measures are reasonable in each case, taking into account the circumstances of the case and always using means that are least intrusive to the privacy of applicants. All of this, subject to the condition that it is a case in which there is *'reasonable doubt'* as to the identity of the applicant.

Page GROUP EUROPE has not justified the existence of such reasonable doubts regarding the complainant's identity. On the contrary, that entity's actions are in accordance with the rights management procedure which it has itself designed, in its capacity as controller, which required the documentation referred to above in all cases, without first analysing whether or not such reasonable doubts were raised.

Nor does the procedure designed by the requested entity provide for the possibility of verifying the identity of the applicant by means of other information or measures other than the provision of supporting documents.

In this case, the complainant was registered in the information systems of the responsible entity, which had extensive information about it; and that the request for access to personal data was made from the same email address of the complainant as was already in the database of the complainant.

It is therefore not understood that this case has been treated as one of those cases where there are doubts as to the identity of the applicant (this is only explained by considering that all the cases of access and portability were thus considered by the respondent); and that, without any other basic approach, PAGE GROUP EUROPE required the provision of several identification documents (those identified), when it had less intrusive means to ensure that the information would be sent to the data subject, such as having checked some of the data already available.

Page GROUP EUROPE was aware of the complainant's contact details, so that the request received from the email address that the entity had registered in its systems and the sending of the requested information with access to that address provided sufficient guarantees, in the opinion of the Agency, to have complied with the request received. Moreover, it has not been established that there was any circumstance that led the requested entity to think of an identity theft or a computer attack.

The strict requirements imposed on the complainant to comply with her request for

access led to the fact that this request was left unanswered, despite the two warnings issued by the complainant herself regarding the excessive requests for documentation sent to her; they determined that the complainant chose to go to the data protection authority of the Netherlands instead of continuing the processing of her application, as she had warned in her email of 11 November 2018.

Consequently, PAGE GROUP EUROPE is responsible for ensuring that the deadline set for responding to the complainant's request elapses without a proper reply, providing it with the requested information.

The right of access was finally granted on 27 August 2020, during the processing of the complaint carried out by this Agency as the lead supervisory authority, following an express request from this Agency dated 14 August 2020. In this regard, it should be pointed out that the response to the request for access cannot be expressed in the context of a mere administrative procedure, such as the forwarding of the complaint to the requested party pursuant to Article 64 (3) of the LOPDGDD.

Consequently, in accordance with the evidence set out above, the aforementioned facts constitute an infringement of Article 12 (2) and (3) of the GDPR, as a result of the failure to take account of the right of access exercised by the complainant, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of that Regulation.

V

In response to the complainant's request for access of 28 September 2018, the responsible entity initially required the complainant to provide two out of three categories of identification documentation: passport, national identity card or driving licence showing date of birth; social security or national insurance card; or invoice for public services aged less than 3 months.

As set out in the previous legal ground, this action by the requested entity responds to the rights management procedure which it has itself designed, as the controller, which required the documentation referred to above in all cases and without considering the possibility of verifying the identity of the applicant by means of information other than the documents referred to above.

The complainant considered that there was no reason to require such identifying information as necessary for the attention of the law, considering that it was not required to open an account on the web portal or to submit its CV. According to the complainant, the authenticated access to the account, which was still active at the time when the request was made to the responsible entity, should be sufficient to understand the exercise of the right and prove her identity in a system such as that used by the controller, based on the use of a private account.

The arguments put forward by the supervisory authorities CNPD and Berlin DPA, mentioned in the Fourth Fact, which have already pointed out that the procedure put in place for the attention of rights do not discriminate against cases where there are doubts as to the identity of the applicant who do not; whereas this procedure does not protect

the data of applicants and increases the risks for those concerned; whereas this documentation is not required from data subjects to open an account or send a CV; additional information should only be requested if there are doubts as to the identity of the data subject, requesting information necessary and appropriate for such verification, on the basis of the applicant's available data.

Both supervisory authorities advocate a less intrusive way of verifying the identity of the applicant, other than the verification of the identity card (e.g. electronic identification or sending the application via the user account together with an additional authentication factor sent via another channel); and agree with the complainant that access to the private account should be understood as sufficient.

They also serve, by coincidence, the arguments set out in the previous legal basis, concerning the possibility of requesting additional information necessary to confirm the identity of the data subject only where the controller has reasonable doubts as to the identity of the applicant for the right (Article 12 (6) GDPR).

PAGE GROUP EUROPE has acknowledged that the identification documentation required from the complainant to verify her identity was required in all cases of exercising rights (at least for requests for access or portability), following the procedure designed by the complainant itself. As stated, it sought to ensure that candidates' personal data were not transferred to third parties who could have access to the credentials of persons registered in their systems for the purpose of deleting their identity and making the application on their behalf, through phishing or social engineering attacks.

In order to assess these facts, account must also be taken of Articles 25 and 32 of the GDPR, which provide that:

'Article 25. Data protection by design and by default.
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article'.

'Article 32. Security of processing.
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the

risk, including inter alia as appropriate:
(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
(…)'

In this case, the system designed by PAGE GROUP EUROPE lays down requirements for the attention of data subjects' rights which go beyond what is provided for in the legislation governing these rights; they do not meet any of the criteria and factors referred to in Article 25 (1) of the GDPR, such as the context, the risks or the purpose of the processing.

Moreover, it is clear that using two of the three documents required by PAGE GROUP EUROPE to verify the identity of the applicants for rights does not guarantee that only personal data that are necessary for this specific purpose are processed.

Against this, the respondent's arguments that the use of those documents is limited to verifying that the applicant's name corresponds to the data available (if that was the case, it is not understood that the date of birth was expressly required), that they are deleted immediately after that check (a fact which has not been proven or was initially stated) and that their access is made solely by the Department of Legal Compliance and, ultimately, the DPO, are insufficient.

The excess, in this case, is apparent simply from the collection of the documents requested by the respondent.

For the same reasons, it is considered that the processing of personal data contained in the identification documents that PAGE GROUP EUROPE requested, in general, from persons making a request to exercise access and portability rights, which were not necessary for the management of that request, increase the risks for those concerned and does not guarantee a level of security appropriate to the risk.

As a result, the provision by any data subject of the documentation required by PAGE GROUP EUROPE in order to verify his or her identity, in the context of a request to exercise the right of access or portability, results, in the circumstances indicated, in the processing of inappropriate, irrelevant and not necessary personal data for this specific purpose of the processing, contrary to the data protection principles, in particular the principle of *'data minimisation'* laid down in Article 5 (1) (c) GDPR:

'Article 5 Principles relating to processing of personal data
1.Personal data shall be:
(*c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')'*.

As regards the scope of that principle, recital 39 of the GDPR states that *'personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means'*.

There is no need to insist on the fact that in the cases analysed there is no need to collect identification documentation from persons applying for a right, as there are other reliable, less intrusive means of identification; the collection of several identity documents is even less necessary.

The respondent required the production of two out of three documents (passport, national identity card or driving licence, showing the date of birth; social security or national insurance card; or invoice for public services aged less than 3 months), and it would not be until the complainant's repeated protest that PAGE GROUP EUROPE considered the request for documentation excessive and corrected to request a copy of a single identification document on both sides. Rectification that does not resolve non-compliance with the data minimisation principle.

The petitioner also considers that the absence of further processing of the data contained in the identification documents, their limited and exclusive use by the legal compliance team makes its action compatible with the principle of minimisation, as it is necessary, proportionate and appropriate to protect the rights of the data subject, thus complying with recital 156 of the GDPR, according to which *'The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles'*.

However, this recital refers to processing for archiving purposes in the public interest and cannot be referred to in the present case.

Consequently, the above-mentioned facts, in relation to the data processing involved in the rights management procedure followed by PAGE GROUP EUROPE for the verification of the identity of the data subjects, constitute an infringement of Article 5 (1) (c) of the GDPR, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of that Regulation.

VI

In the event of an infringement of the provisions of the GDPR, among the corrective powers available to the Spanish Data Protection Agency as the supervisory authority, Article 58 (2) of the GDPR provides for the following:

'2 each supervisory authority shall have all of the following corrective powers:
(...)
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;'
(...)
(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(...)

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;'

According to Article 83 (2) GDPR, the measure provided for in point (d) above is compatible with the penalty consisting of an administrative fine.

VII

The facts set out above do not comply with the provisions of Articles 12 and 5.1 (c) of the GDPR, with the scope set out in the preceding legal bases, which entails the commission of infringements set out in Article 83 (5) (b) and (5) (a) of the GDPR, which, under the *heading 'General conditions for the imposition of administrative fines*', provides as follows:

'5. 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:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9.
(b) the data subjects' rights within pursuant to Articles 12 to 22'.

In this regard, Article 74 of the LOPDGDD considers that infringements of a purely formal nature of the articles referred to in Article 83 (5) of the GDPR and, in *particular, '(c) failing to attend to the requirements to exercise any of the rights established by Articles 15 to 22 of Regulation (EU) 2016/679, unless this results from the implementation of Article 72 (1) (k) of this Organic Law', is regarded as a 'minor' infringement* for the purposes of limitation period.

For its part, Article 72 (1) (a) of the LOPDGDD considers, for the purposes of limitation period, *as 'very serious*':

'1. 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:

(a) The processing of personal data which infringes the principles and guarantees provided for in article 5 of Regulation (EU) 2016/679.'

In order to determine the administrative fine to be imposed, it is necessary to comply with the provisions of Articles 83.1 and 83.2 of the GDPR, which state**:**

'1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
(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;

(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.'

Article 76 of the LOPDGDD, entitled *'Penalties and corrective measures'*, provides:

'1. Penalties provided by sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679 shall apply considering their degree and the criteria established in section 2 of the aforementioned article.
2. Pursuant to the provisions of article 83.2.k) of Regulation (EU) 2016/679, the following criteria may also be considered:

(a) The ongoing nature of the relevant infringement.
(b) The existence of a link between the perpetrator's activities and their processing of personal data.
(c) Any profits obtained as a consequence of the relevant infringement.
(d) The possibility that the perpetrator's activities have induced them to commit the relevant infringement.
(e)The existence of a merger by acquisition subsequent to the infringement, which may not be attributed to the acquiring company.
(f) Whether the rights of minors have been affected.
(g) The existence of a Data Protection Officer, in those cases when their appointment is not compulsory'.
(h) Voluntary submission by the data processor or the data controller to alternative dispute resolution methods, in those cases in which disputes arise between the data processor or the data controller and any other stakeholder.'

In this case, having regard to the gravity of the infringements found, it is appropriate to impose a fine and, where appropriate, to adopt measures. The request made by PAGE GROUP EUROPE for the imposition of other corrective powers, such as the reprimand, which is provided for natural persons and where the penalty constitutes a disproportionate burden, cannot be accepted (recital 148 GDPR). In this regard, the Agency does not agree that the infringements found are of minor gravity, taking into account the effects they have had on the exercise of the rights granted to data subjects; nor the short duration claimed by the respondent, given that the irregular process of managing those rights has been imposed since the time when the GDPR became applicable.

In accordance with the above provisions, for the purpose of determining the amount of the penalties to be imposed in the present case, it is considered that the fines should be graduated according to the following criteria:

1. Infringement of Article 12 of the GDPR, defined in Article 83 (5) (b) and classified as minor for the purposes of limitation in Article 74 (c) of the LOPDGDD:

The following criteria for graduation are considered to be aggravating factors:

. Article 83 (2) (a) GDPR: '*(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.*

. The nature of the infringement, in that the lack of attention to the right of access, due to its content, affects the complainant's ability to exercise genuine control over her personal data.
. The nature of the harm caused to the data subject, who was deprived of one of her basic rights with regard to the protection of personal data, despite the communications sent by the data subject, insisting on his or her interest.

. Article 83 (2) (d) GDPR: *"(D) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32.'*

The entity charged does not have adequate procedures in place to act on the collection and processing of personal data, as regards the management of requests for the exercise of rights, so that the infringement is not the result of an anomaly in the operation of those procedures but of a defect in the personal data management system designed by the controller. That procedure was adopted by the defendant on its own initiative laying down requirements going beyond the applicable legislative provisions.

. Article 76 (2) (b) of the LOPDGDD: *"(b)The existence of a link between the perpetrator's activities and their processing of personal data'.*

The fact that the infringer's activity is closely linked to the processing of personal data, taking into account the activity it carries out in the human resources sector and the level of establishment of the entity (Sixth Fact contains some details on this implementation).

. Article 83 (2) (k) GDPR: *"(K) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."*

The status of large enterprise and turnover of PageGroup and PAGE GROUP EUROPE (see Sixth Fact for some details).

The following circumstances are also considered to be mitigating:

. Article 83 (2) (f) GDPR: *"(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement".*

The right of access exercised by the complainant was ultimately granted by the requested entity, although the intervention of the supervisory authorities was required.

PAGE GROUP EUROPE, in its written pleadings, did not make any statement regarding the criteria and factors assessed for grading this infringement.

In view of the factors set out above, the assessment of the fine for infringement of Article 12 of the GDPR is 50,000 EUR (fifty thousand euros).

2. Infringement for failure to comply with the provisions of Article 5 (1) (c) of the GDPR, defined in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (a) of the LOPDGDD:

The following criteria for graduation are considered to be aggravating factors:

. Article 83 (2) (a) GDPR: *"(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'*

. The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operations concerned. The infringement concerns fundamental aspects of data protection and results in the processing of identification documents of data subjects, in accordance with the rights management procedure that implemented the requested person at the time when the GDPR became applicable, which has not been rectified until the opening of the procedure.
. The number of data subjects affected: the infringement concerns all data subjects who have exercised the right of access or portability, although it is necessary to consider the significance that the infringing conduct may have had on all of the entity's customers, many of them considering the level of international implementation of the infringement.
. The nature of the damage caused to the data subjects, who have seen their rights limited and the risk to their privacy increased.

. Article 83 (2) (b) GDPR: *'(b) the intentional or negligent character of the infringement'*.

The negligence found to have been committed in committing the infringement.

In that regard, the argument put forward by PAGE GROUP EUROPE that negligence must be assessed when the conduct deviates from recognised standards cannot be accepted. If an action deviates from the standard, it cannot be said that it meets the standards.

Furthermore, in relation to the complainant's request for access, despite the complainant's allegations that the documentation requested from it was excessive, it continued to request that documentation and did not comply with the right until the intervention of the supervisory authorities.

. Article 83 (2) (d) GDPR: *'(D) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32.'*

The entity charged does not have adequate procedures in place for the collection and processing of personal data, so that the infringement is not the result of an anomaly in the operation of those procedures but of a defect in the personal data management system designed by the controller.

. Article 76 (2) (a) of the LOPDGDD: *'(a) the ongoing nature of the relevant infringement'*.

The rights management procedure put in place by the respondent applied to all requests to exercise access and portability rights that customers have made since the GDPR became applicable. This is a number of actions following the action designed by PAGE GROUP EUROPE, which infringe the same provision.

. Article 76 (2) (b) of the LOPDGDD: *'(b) the existence of a link between the perpetrator's activities and their processing of personal data'.*

The fact that the activity of the infringer is closely linked to the processing of personal data, taking into account the reasons already expressed when setting out the factors used to determine the scale of the previous infringement.

. Article 83 (2) (k) GDPR: *'(K) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, through the infringement.'*

. The volume of data and processing that is the subject of the file, taking into account the level of information requested from persons accessing its services.
. The status of large enterprise and turnover of PageGroup and PAGE GROUP EUROPE.

The following circumstances are also considered to be mitigating:

. Article 83 (2) (c) GDPR: *'Any action taken by the controller or processor to mitigate the damage suffered by data subjects'.*
. Article 83 (2) (f) GDPR: *'The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement'.*

PAGE GROUP EUROPE has designed a new rights management procedure to remedy the concerns that have led to infringements being committed. However, it should be borne in mind that this remedy did not take place until after the procedure had been opened.

In view of the factors set out above, the assessment reached by the fine for infringement of Article 5 (1) (c) of the GDPR is 250,000 EUR (two hundred and fifty thousand euros).

None of the graduation factors considered is mitigated by the fact that the requested entity has not previously been the subject of penalty proceedings, a fact which has been invoked by the requested entity to be considered a mitigating factor.

In this regard, the judgment of the NA of 05 May 2021, rec. 1437/2020, states that *'It also considers that the failure to commit an earlier infringement should be regarded as mitigating. Article 83 (2) of the GDPR provides that account must be taken of, inter alia, '(e) any previous infringement committed by the controller or processor' for the purposes of imposing the administrative fine. This is an aggravating circumstance, the fact that the budget for its application is not met means that it cannot be taken into consideration, but does not imply or permit, as the applicant claims, its application as an attenuating factor.'*

PAGE GROUP EUROPE also refers in its submissions to two actions taken by the data protection authority of the Netherlands for illegal processing of identity documents in which the companies concerned were not penalised, although, according to the requested entity itself, these are actions prior to the entry into force of the GDPR. Furthermore, the details which determined those agreements are not provided.

VIII

Infringements may result in the controller being required to *take appropriate measures to bring its action in line with the rules referred to in this act, in accordance with the aforementioned Article 58 (2) (d) GDPR, according to which each supervisory authority may 'order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period'.* Failure to comply with this body's requirements may be regarded as a serious administrative offence because it *'does not cooperate with the supervisory authority'* in response to such requests, and such conduct may be assessed when administrative proceedings are initiated with a pecuniary fine.

In such a case, in the decision to be adopted, the Agency may require the entity responsible to comply, within a period to be determined, with the rules on the protection of personal data, the processing operations it carries out and the mechanisms and procedures it follows to meet requests for the exercise of rights made to it by data subjects, to the extent set out in the legal bases of this Agreement.

Likewise, the measures which may be taken in the decision terminating the proceedings, in relation to processing activities and the exercise of rights, shall apply in all the countries of the European Union in which PageGroup operates.

In this case, following the complainant's complaint, which considered the documentation required to prove her identity to be excessive when exercising the right of access, the responsible entity corrected and requested only a copy of the identification document on both sides.

In addition, PAGE GROUP EUROPE, when the complaint was sent, stated that it *'has abolished the procedure whereby two out of three categories of identification documentation were requested. At present, PAGE only requests an identification document and also offers alternatives to interested parties, such as signing by means of*

an electronic certificate, face-to-face care in any office of PageGroup or any other means which the person concerned considers appropriate'.

In that regard, it provides a copy of the *'Reply Models'* used at that date to verify the identity of the data subjects. The first of these requests the data subject to copy the identity card or EIN, passport or driving licence with date of birth, any of them; attention is also drawn to the possibility of using alternative means, should the data subject prefer not to send such documents. The second model refers to such alternative means, such as the presence in a Group office or the sending of a document signed by means of an electronic certificate.

These measures represent an improvement compared to the procedure initially followed, the one applied to the complainant, which required two identification documents and not only one, but did not fully correct the concerns raised in this act.

However, in its written pleadings to the opening of the procedure, the aforementioned entity provided the document entitled *'EU GDPR Data Request Process'*, which sets out the way in which it is currently dealing with requests for the exercise of rights. This new process abandons the practice of requiring identification documents for the purpose of dealing with access requests, which validate only by means of the applicant's first name, surname and e-mail and his/her match with those registered in his/her information system.

It also sets out the cases in which additional information should be required, where there are reasonable doubts as to the identity of the applicant, in cases where there are several persons with the same name or in case of duplication/doubt about the e-mail address. In such cases, it intends to send an email to the data subject requesting information already contained in the applicant's profile registered in his or her database, and cites as an example the postcode or the last three digits of his or her telephone number.

In addition, it provides for alternative means to enable the person concerned to prove his/her identity, in the event that he/she is unwilling to provide the additional information (to be presented to a PageGroup office or to send a document bearing a digital signature; or communicate whether it has a different means); it has planned not to process any identity document it might receive, by deleting it immediately.

It is considered that these new measures implemented by PAGE GROUP EUROPE comply with the criteria assessed in these actions, in relation to the procedures for managing applications for the exercise of rights and the means of validating the identity of applicants, and it is not appropriate to impose additional measures.

IX

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

"1. Once penalty proceedings have been initiated, if the offender recognises his liability, the proceedings may be resolved by the imposition of the appropriate penalty.

2. Where the penalty is solely of a financial nature or where a financial penalty and a financial

penalty of a non-pecuniary nature may be imposed but the second penalty is justified, voluntary payment by the person presumed to be liable, at any time prior to the decision, shall lead to the termination of the proceedings, except as regards the restoration of the situation which has been altered or the determination of compensation for the damage caused by the commission of the infringement.

3. In both cases, where the penalty is purely financial in nature, the body responsible for deciding the procedure shall apply reductions of at least 20 % of the amount of the penalty proposed, which are cumulative with each other. Such reductions shall be determined in the notification of initiation of proceedings and their effectiveness shall be subject to withdrawal or waiver of any administrative action or appeal against the penalty.

The percentage reduction provided for in this paragraph may be increased by regulation'.

The entity PAGE GROUP EUROPE, during the period granted to it to submit arguments on the proposal for the resolution, proceeded to voluntarily pay the penalty with the reduction provided for by law, which determines the end of the procedure and renounces any administrative action or appeal against the penalty.

Therefore, in accordance with the applicable legislation, the Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Declare the termination of proceedings PS/00003/2021 against PAGE GROUP EUROPE, S.L. for infringements of Articles 12 and 5.1 (c) of the GDPR, as set out in Articles 83.5 (b) and 83.5 (a) of that regulation respectively; in accordance with Article 85 of the LPACAP.

SECOND: Notify this resolution to PAGE GROUP EUROPE, S.L.

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

In accordance with the provisions of (48.6) and (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 Jurisdiction, within two months of the day following notification of this act, in accordance with Article 46 (1) of that Law.

938-231221

Mar España Martí
Director of the Spanish Data Protection Agency