

APPEAL FOR REVERSAL

Before the administrative court

Case *noyb* (for [REDACTED]) / CNPD

Article 78 of the General Data Protection Regulations

To the Presidents and Judges composing the Administrative Court of and in Luxembourg,

The association under Austrian law *noyb - European Center for Digital Rights*, registered with the *Zentrales Vereinsregister* under number 1354838270, with registered office at Goldschlagstraße 172/4/3/2, AT-1140 Vienna, Austria (Exhibit 1 - extract from the register of associations "Vereinsregister") commissioned by [REDACTED] residing at [REDACTED] (cf. Exhibit 2, Representation Agreement),

That by the present, the applicant hereby files an **action for reversal if not annulment** before Your Administrative Court against a decision of the National Commission for Data Protection (hereinafter "CNPD") of 18 September 2020 (Exhibit 3).

IN FACT

RocketReach describes itself as follows on the home page of its website <https://rocketreach.co> (Exhibit 4, site home page): "*Real-time verified data for 450 million professionals across 17 million companies, worldwide. Trusted by over 6.7 million users - powering sales, recruiting, and marketing at companies large and small. Prospect, connect and converse with your leads at scale.*" In other words, this company (based in the United States at 10400 NE 4th St #23, Bellevue, WA 98004 according to the information available on its website) collects and markets data on professionals from all over the world, including the European Union.

On April 5, 2019, [REDACTED] having noted that RocketReach has collected personal data concerning him, contacts this company at the address indicated on its website. Relying on Article 15 of the General Regulation on Data Protection (Regulation 2016/679 of 27 April 2016, hereinafter "GDPR"), he requested information on the processing of his data by RocketReach, in accordance with Article 15 (1) of the GDPR (Exhibit 5: exchange of emails of 5 April 2019). Thus, for example, [REDACTED] asks RocketReach to inform it of the purpose of the processing carried out, the categories of data collected concerning it, or the period for which the data was to be kept. [REDACTED] did not request the copying or deletion of its data, as it could have done in accordance with Articles 15 (3) and 17 of the GDPR.

On the same day, RocketReach replied to [REDACTED] by attaching a copy of the data concerning him and indicating in particular that it has deleted the personal data concerning him from its databases (still [Exhibit 5](#)).

Noting that RocketReach is avoiding responding to its requests, [REDACTED] addresses a claim to the CNPD ([Exhibit 6](#), Claim).

On 9 April 2019, the CNPD acknowledges receipt of [REDACTED]'s claim and requests additional information from him, which he provides on the same day ([Exhibit 7](#), exchange of emails).

On May 14, 2019, [REDACTED] sends a new email to the CNPD to request news of his claim. It is only after a telephone reminder that he receives an answer, on 11 July 2019, indicating that his claim is still being processed ([Exhibit 8](#), exchange of emails).

[REDACTED] then sends further reminders by email on 26 September 2019, 27 October 2019, then again on 4 November 2019, before finally receiving a reply on the same day informing him that his complaint is still being examined ([Exhibit 9](#)).

By email of 6 March 2020 ([Exhibit 10](#)), the CNPD informs [REDACTED] that it is *"impossible for it to proceed any further with the processing of [its] claim"* and to *"effectively continue the processing of [its] file"*. *"Indeed, it states that RocketReach has informed it "that it considers that it is the users of its services, and not itself, who are responsible for processing personal data". The CNPD also indicates that it emerges from the instruction that RocketReach "is a company located in the United States of America which does not have a representative in the Union within the meaning of Article 27 of the GDPR". The CNPD also confirms that it does not share RocketReach's point of view and is "on the contrary of the opinion that this company is indeed to be considered as a data controller for the processing of personal data carried out on its website". However, on the other hand, the CNPD concludes that it does not have "the powers to carry out investigations and to enforce the decisions that we would be led to take on the territory of the United States of America. "For these reasons, the CNPD is discontinuing the processing of the case of [REDACTED].*

[REDACTED] replies by email ([Exhibit 11](#)) asking whether he understands that *"the CNPD will not take action"* in his file.

On 17 March 2020 (still [Exhibit 11](#)), the CNPD reiterated its response in the following terms: *"we consider that we will not be able to effectively pursue the processing of your claim, given the limits of our powers of investigation and enforcement of decisions that we may have to take on the territory of the United States of America. »*

Several emails from [REDACTED] followed, asking for further details and asking in particular about the existence of organisations likely to assist him at European level to follow up on his approach ([Exhibit 12](#): emails of 17 March 2020, 28 March 2020, 19 April 2020, 26 April 2020).

On 4 May 2020, [REDACTED] sent a registered letter to the President of the CNPD deploring the Commission's lack of responsiveness on the claims lodged with it ([Exhibit 13](#)).

The CNPD replied succinctly by email on 25 May 2020, stating in particular: "To our knowledge, there is no European organisation with the competence to take binding decisions against RocketReach in terms of personal data protection." (Exhibit 13).

On 29 May 2020, ██████████ requests a signed decision, invoking Articles 12 and 13 of the Rules of Procedure of the CNPD (Exhibit 15).

On 8 July 2020, the CNPD replied that these provisions "do not apply in this case. Indeed, this case concerns a claim, which was not the subject of a decision taken in a deliberation session of the CNPD within the meaning of these articles. ». She added: "Please note that the CNPD has taken note of your claim, and informed you of its progress and outcome in accordance with Articles 57(1)(f), 77(2) and 78(2) of the GDPR, in particular through our last emails of 6 March, 17 March and 25 May 2020, to which we refer you." (Exhibit 16).

██████████ sent another registered letter to the President of the CNPD on 10 August 2020 (Exhibit 17) before finally obtaining a letter signed by a Commissioner of the CNPD on 18 September 2020 (Exhibit 3, the decision undertaken).

The letter reads as follows:

██████████,

The (CNPD) returns to your email of July 8, 2020 regarding your claim of April 5, 2019 against RocketReach.

With regard to your request for clarification on the reasons why Articles 9 of the CNPD's Rules of Procedure for Investigations (hereinafter the "Investigation Rules") and Articles 10 and 12 of the CNPDs Internal Rules of Procedure (hereinafter the "ROI") do not apply in this case, we would like to inform you that it is clear from the Rules of Procedure that investigation and complaint files are subject to different procedures.

The Investigation Regulation is only applicable to investigation files, and Articles 10 and 12 of the ROI mentioned above are only applicable to the deliberation sessions of the CNPD, including deliberations on investigation files.

Moreover, although the processing of a complaint may lead to the proposal and opening of an investigation in accordance with the procedures laid down in Article 2 of the Inquiry Regulation, the opening of an investigation file following a complaint is not systematic.

Indeed, when a complaint is lodged, the "complaints" department tries to resolve the problem raised without opening a formal investigation within the meaning of Articles 37 to 41 of the Act of¹ August 2018 organising the CNPD and the general data protection regime (hereinafter: "Act of¹ August 2018"). Most complaints can be resolved and closed in this way, after the CNPD has intervened with the controller concerned. When it turns out that the file of a complaint cannot be investigated in this way, the Council may decide to open an investigation.

There are no legislative criteria that define when the CNPD should or should not open an investigation. The CNPD is an independent supervisory authority which benefits from the principle of "opportunity for action" (cf. Opinion of the Council of State of 26 June 2018, doc. parl. N°7184/28). It may also refuse to act on a complaint which is manifestly unfounded or excessive, in accordance with Article 57 (4) of the GDPR.

In the case of your complaint, the opening of an investigation file does not appear relevant, as the CNPD has no means of action against a controller established on the territory of the European Union (EU) or which has not appointed a representative in the EU under Article 27 of the GDPR. Indeed, in these cases, it is impossible for the controller to enforce the provisions of the GDPR on the territory of the United States of America.

Considering that we have answered your questions, we consider that our intervention in the context of your complaint is now over.

(...) »

It is against this decision that the applicant lodges the present appeal.

ON THE RIGHT

I. Admissibility

A. Representation agreement

Article 80(1) of the GDPR entitled "**Representation of the persons concerned**" provides that :

The data subject shall have the right to instruct a non-profit-making body, organisation or association which has been duly constituted in accordance with the law of a Member State, whose statutory objectives are in the public interest and which is active in the field of the protection of the rights and freedoms of data subjects in the context of the protection of personal data concerning them, to bring a claim on his behalf, exercise on his behalf the rights referred to in Articles 77, 78 and 79 and exercise on his behalf the right to obtain compensation referred to in Article 82 where the law of a Member State so provides.

Precisely, the plaintiff, having already brought several proceedings in different Member States on the basis of this provision, fulfils all these criteria:

- it is a non-profit-making association (§2 of the statutes (room 18): "*Der Verein, dessen Tätigkeit nicht auf Gewinn gerichtet ist...*")
- the association, which has its seat in Vienna, is validly constituted under Austrian law (§1(4) of the statute and Exhibit 1)
- its statutory objectives are in the public interest and the association acts in the field of personal data protection: "*Der Verein, (...) bezweckt die Förderung der Allgemeinheit auf den Gebieten der Freiheit, der Demokratie und des Konsumentenschutzes im digitalen Bereich mit Schwerpunkt auf Verbraucherrechte, die Grundrechte auf Privatsphäre und Selbstbestimmung, Datenschutz, Meinungsfreiheit, Informationsfreiheit, Menschenrechte sowie das Grundrecht auf einen wirksamen Rechtsbehelf. The association also aims to promote relevant adult education (popular education), research and science*" et "*The association pursues these purposes objectively, independently, and exclusively and directly on a non-profit basis (...)*" (§2(1) et §2(2) of the statute).

In addition, [REDACTED] signed a Representation Agreement (Exhibit 2) giving *noyb* a mandate to exercise on its behalf the rights referred to in Articles 77, 78 and 79 of the GDPR.

Consequently, the applicant is admissible to act to enforce the rights of [REDACTED] namely to appeal against a decision of a supervisory authority, as provided for in Article 78 of the GDPR.

B. Right to an effective remedy against the decisions of the CNPD

Article 47(1) of the Charter of Fundamental Rights of the European Union enshrines the right of everyone whose rights and freedoms guaranteed by Union law have been infringed to an effective remedy before a court of law.

The right to protection of personal data is guaranteed by Union law, specifically by Article 8 of the Charter of Fundamental Rights, paragraph 3 of which states that compliance with the rules giving effect to this right "*shall be subject to control by an independent authority.* »

Article 78(2) of the GDPR provides :

2. *Without prejudice to any other administrative or extrajudicial **remedy, any person concerned shall have the right to seek an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 fails to deal with a complaint or to inform the person concerned within three months of the progress or outcome of the complaint he or she has lodged under Article 77.***

This provision should be read in the light of recital 143 of the GDPR, which states that "***any natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects for that person. Such a decision concerns in particular the exercise by the supervisory authority of powers of investigation, adoption of corrective measures and authorisation or refusal or rejection of complaints. (...) Proceedings against a supervisory authority should be brought before the courts of the Member State on whose territory the supervisory authority is established and be conducted in accordance with the procedural law of that Member State. Those courts should have full jurisdiction, including the power to examine all questions of fact and law relating to the dispute before them.*** »

Thus, any decision adopted by the CNPD in the exercise of its powers, in particular in the context of the processing of complaints within the meaning of Article 77 of the GDPR, must be subject not only to an appeal but also to an appeal of full jurisdiction, in other words an appeal for reversal.

Moreover, the so-called "*Schrems II*" judgment of the European Court of Justice (ECJ, 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559) clarified the scope of the obligations of national data protection authorities in these terms (paragraph 109 of the judgment): "*under Article 57(1)(f) of the GDPR, each supervisory authority is required, within its territory, to deal with complaints which any person is entitled to make pursuant to Article 77(1) of that regulation where he considers that a processing of personal data relating to him constitutes a breach of that regulation, and to investigate the matter to the extent necessary. The supervisory authority must deal with such a complaint with all due diligence (...).* »

However, as the Court again points out, recital 141 of the GDPR refers to the "*right to an effective judicial remedy in accordance with Article 47 of the Charter*" in the event that the supervisory authority "*fails to act when action is necessary to protect the rights of the person concerned*". (paragraph 110 of the judgment)

Thus, the right to an effective judicial remedy as protected by Union law is reflected in the right to a remedy in cases where a supervisory authority fails to exercise due diligence to protect the rights of the data subject, in particular in the context of the implementation of Article 77 of the GDPR.

The principles of Union law set out above are expressly confirmed by the national law transposing them. Thus, Article 55 of the Act of 1 August 2018 on the organisation of the National Commission for Data Protection provides: "*An appeal against the decisions of the CNPD taken pursuant to this Act shall be brought before the Administrative Court, which shall rule as the court of first instance.* »

In addition, the CNPD Rules entitled "*Procedure for Claims before the CNPD*" take these requirements into account as they contain the following provisions.

Article 7 provides that: "*(...) When, after analysis, the CNPD comes to the conclusion that the claim is unfounded, it shall inform the parties by a letter containing the reasons for its position.* »

Article 9 reads as follows:

"The CNPD may decide : (1) to close a case on the basis of Article 3 of the present procedure, (2) to close a file at the end of the investigation of the complaint carried out in accordance with Article 7 of the present procedure.

*In such cases, **the CNPD notifies the claimant of its decision to close the file or to close the file and informs him that he may** (...) pursuant to Article 78 of the GDPR, Article 55 of the Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the general data protection regime (...) lodge **an appeal for reversal before the administrative court within 3 months of the notification of the decision.** »*

Accordingly, pursuant to Article 78 of the GDPR, Article 55 of the Act organising the CNPD and Article 9 of the Rules of Procedure relating to claims before the CNPD, the present application for reversal is to be declared admissible.

In the alternative, Your Tribunal is requested to declare admissible the action for annulment brought against the decision taken, pursuant to Article 2(1) of the amended Act of 7 November 1996 on the organisation of administrative courts.

C. Time limit for appeal

It follows from the aforementioned Article 9 of the Rules of Procedure for claims before the CNPD that the CNPD had to indicate to [REDACTED] that an appeal for reversal could be lodged with the administrative court within 3 months of notification of the decision taken. This requirement is in accordance with Article 14 of the Grand-Ducal Regulation of 8 June 1979 on the procedure to be followed by administrations under the State and the

municipalities, which requires the administration to inform the constituent of the means of appeal against a decision.

However, according to settled case law, the administration's failure to inform the constituent of the means of appeal against an administrative decision means that the time limits set for appeals do not begin to run (cf. for example Trib. adm., 18 November 2009, no. 25455 of the roll, citing Trib. adm., 7 February 2002, no. 13136 of the roll confirmed by CA 14 May 2002, no. 14676C of the roll and other decisions cited in *Pas. adm.* 2008, V° PANC, no. 166).

In the present case, the decision taken does not mention any means of appeal or time limits for appeal, so that the time limit for appealing against this decision never began to run.

The appellant therefore requests Your Court to find the application admissible.

II. **As to the merits: violation by the CNPD of Article 57 of the GDPR relating to the tasks of the supervisory authorities, of its duty of diligence, and of Articles 27 and 15 of the GDPR**

The email of 6 March 2020 (Exhibit 10) provides important elements as to the motivations behind the decision taken. The CNPD states in this email that the company RocketReach communicated to it "*that it considers that it is the users of its services, and not itself, who are the data controllers with regard to personal data*". The CNPD admits that it does not share this point of view: it is "*on the contrary of opinion that this company is indeed to be considered as the data controller for the processing of personal data carried out on its website.*" »

The CNPD also states that it appears from the Instruction that RocketReach "is a company located in the United States of America which does not have a representative in the Union within the meaning of Article 27 of the GDPR". The Commission therefore accepts that RocketReach is indeed subject to the GDPR and that it continues its activities in violation of the GDPR, or at least in violation of Article 27 of the GDPR.

In spite of this observation, the CNPD announces to ██████████ that it is impossible for it to "*effectively pursue*" the processing of its file. This conclusion will be formally reiterated in the decision taken on 18 September 2020: "*the opening of an investigation file does not appear relevant, as the CNPD has no means of action against a data controller established on the territory of the European Union (EU) or having not appointed a representative in the EU pursuant to Article 27 of the GDPR. Indeed, in these cases, it is impossible for the controller to enforce the provisions of the GDPR on the territory of the United States of America.*" »

This reasoning already gives rise to two general objections.

Firstly, the fact that a natural or legal person does not appear in proceedings brought against it does not prevent such proceedings from being conducted, provided that certain guarantees are respected and in particular that the public authority or private person initiating such proceedings is diligent and endeavours to contact the person concerned. This applies not only in administrative matters (in the absence of updated information from a taxable person, the tax authorities proceed with taxation *ex officio*), but also in civil proceedings (the judge may

give judgment in the absence of the defendant once the plaintiff has complied with the applicable rules on service) and even in criminal proceedings. The lack of cooperation of the company concerned is therefore insufficient to justify its inaction.

Secondly, even if it were to be shown to be difficult or impossible in practice to apply any measures or sanctions decided by the CNPD, this cannot be used as an excuse to refrain from taking such measures. The appropriateness of the decisions of the CNPD is to be assessed not in terms of their ease of implementation but in terms of the applicable legislation.

However, the explanations provided by the CNPD in the email of 6 March 2020 and in its letter of 18 September 2020 only highlight the illegality of its decision with regard to the GDPR.

A. The missions of the CNPD under Article 57 of the GDPR

First of all, pursuant to Article 7 of the Law of 1 August 2018 on the organisation of the CNPD, "*The CNPD shall carry out the tasks entrusted to it under Article 57 [of the GDPR]*". This provision of the GDPR entrusts national supervisory authorities such as the CNPD with a number of tasks. In particular, the CNPD:

a) ***shall monitor the application of this Regulation and ensure compliance with it***

(...)

f) ***deal with complaints lodged by a data subject or by a body, organisation or association in accordance with Article 80, examine the subject matter of the complaint, to the extent necessary, and inform the complainant of the progress and outcome of the investigation within a reasonable period of time, in particular whether further investigation or coordination with another supervisory authority is necessary***

h) ***carry out investigations into the application of this Regulation, including on the basis of information received from another supervisory authority or public authority***

Thus, under Article 57 of the GDPR, the primary role of the CNPD is to monitor the application of and ensure compliance with the GDPR, which it does in particular by dealing with claims which give rise to fears of a violation of the GDPR and by carrying out investigations.

In carrying out those tasks, the "*opportunity to act*" relied on by the CNPD to justify its inaction in the present case (Exhibit 3 - decision taken, p. 2) is not absolute and cannot allow the CNPD to opt for inaction in the face of a manifest violation of the GDPR and of the rights of a person who has lodged a complaint. Moreover, this principle is not formulated as such in the GDPR and is only derived from an opinion of the Council of State, i.e. of a national advisory authority whose opinion can in no way hinder the proper implementation of Union law, including the provisions of the GDPR and the right to an effective judicial remedy.

It should also be noted that the CNPD invokes in the decision undertaken Article 57(4) of the GDPR according to which it would be entitled to "*refuse to deal with a claim which is manifestly unfounded or excessive*". However, that same provision states that "*the onus is on the supervisory authority to show that the claim is manifestly unfounded or excessive*",

which the CNPD remains in default of doing. On the contrary, the CNPD itself acknowledges the applicability and violation of the GDPR by RocketReach.

B. The applicability of the GDPR to the case at hand

Article 3(2) of the GDPR provides :

"« 2. *This Regulation shall apply to the **processing of personal data relating to data subjects who are within the territory of the Union by a controller or processor not established within the Union, where the processing activities are related:***

- a) *the supply of goods or services to such persons concerned within the Union, whether or not payment is required from them; or*
- b) ***monitoring the behaviour of such persons, insofar as it takes place within the Union.*** »

In the present case, it should be recalled that RocketReach presents itself as follows (Exhibit 4, site home page): "*Real-time verified data for 450 million professionals across 17 million companies, worldwide. Trusted by over 6.7 million users - powering sales, recruiting, and marketing at companies large and small. Prospect, connect and converse with your leads at scale.*" For example, this company collects and markets personal data, including data relating to the professional activities of EU residents, to enable its customers to identify potential customers themselves. This data processing therefore falls within the scope of the GDPR.

Ajoutons que la société RocketReach reconnaît elle-même l'applicabilité du GDPR à son activité : cela ressort de la " GDPR Notice " disponible sur son site internet (pièce 19), dont le point 2 indique notamment : "*RocketReach is subject to GDPR regulations with regards to any RocketReach-processed or controlled data that qualifies for the GDPR protections afforded to personal data originating within the EU and to the individuals having rights to that personal data.* »

Thus, the applicability of the GDPR to the case at hand is not in doubt.

C. Violation of Article 27 of the GDPR by the data controller

By finding that RocketReach, a US-based company, has not "*appointed a representative in the EU under Article 27 of the GDPR*", the decision taken implicitly recognises that there is a breach of a provision of the GDPR, namely Article 27 which reads as follows: "*Where Article 3(2) applies, the controller or processor shall designate in writing a representative in the Union.* »

However, the logic of Article 27, read in conjunction with Article 3(2) mentioned above, is precisely to assure individuals within the European Union that the level of protection of their personal data does not diminish when these data are processed by entities based outside the Union.

Contrary to the reading of the CNPD of this provision, the obligation for a controller established outside the Union to appoint a representative on the territory of the Union is indeed an *obligation within the meaning of Article 27 of the GDPR*, and not a *condition for the territorial application of the GDPR*. Compliance with this obligation must be monitored and its violation must be sanctioned, in particular by the national data protection supervisory

authorities, otherwise Article 27 will be rendered meaningless. The CNPD cannot hide behind an alleged lack of means to evade this legal obligation incumbent on it.

D. Violation of Article 15 of the GDPR by the data controller

The same reasoning applies to RocketReach's equally clear violation of at least one other provision of the GDPR, namely Article 15, which provides for the right of access to data and reads as follows:

- 1) *The data subject shall have the right to obtain confirmation from the controller whether or not personal data concerning him/her are processed and, if so, access to such personal data and the following information:*
 - a) *the purposes of the treatment;*
 - 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 established in third countries or international organisations;*
 - d) *where possible, the intended period of retention of personal data or, where this is not possible, the criteria used to determine this period;*
 - e) *the existence of the right to request the controller to rectify or erase personal data, or a restriction on the processing of personal data relating to the data subject, or the right to object to such processing;*
 - f) *the right to lodge a complaint with a supervisory authority;*
 - g) *where 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, as referred to in Article 22(1) and (4) and, at least in such cases, relevant information concerning the underlying logic and the importance and intended 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, with respect to such transfer.*
- 3) *The controller shall provide a copy of the personal data being processed. The controller may require the payment of a reasonable charge based on administrative costs for any additional copy requested by the data subject. Where the data subject submits his or her request by electronic means, the information shall be provided in a commonly used electronic form unless the data subject requests otherwise.*

However, it should be recalled that when ██████████ sought to obtain the information referred to in Article 15(1) of the GDPR, RocketReach merely replied that it had deleted its data and sent it a copy of the data in question ([Exhibit 4](#), exchange of e-mails). However, ██████████ not request to exercise its right to erase the data (Article 17 of the GDPR) nor its right to obtain a copy of the data (Article 15(3) of the GDPR): it only asked to obtain the information relating to the data processing of which it was the subject, as permitted by Article 15(1) of the GDPR. His request remained unanswered. At the very least, it was incumbent on the CNPD to investigate this violation.

E. The failure of the CNPD to meet its obligations

Having found that RocketReach has not appointed a representative as required by Article 27 of the GDPR, the CNPD concludes that it does not have "*the powers to conduct investigations and to enforce decisions that we would be required to take on the territory of the United States of America*".

Certainly, the CNPD has contacted the company RocketReach. However, RocketReach indicated that it did not consider itself to be a data controller and the CNPD, while disagreeing with this position, decided to stop processing the file in view of the absence of a designated representative on the territory of the Union.

Following the reasoning of the CNPD, it would be sufficient for any data controller to remain established outside the Union, especially not to appoint a representative in the EU, and not to respond to requests from a supervisory authority in order to never be worried and not be subject to any measure decided by an authority of the Union. Such a conception of the competences and powers of supervisory authorities would hinder the effectiveness of the GDPR and deprive individuals of the protection guaranteed to them by the Regulation. It is clear that a mere attempt to make contact falls far short of the means available to the CNPD to investigate a violation of the GDPR. The decision of the CNPD not to use these means is therefore contrary to the spirit and letter of the GDPR.

In support of this conclusion, the CNPD quotes an extract from recital 116 of the GDPR, which states that national data protection authorities "may be faced with the impossibility of examining complaints or conducting investigations into activities carried out outside their borders. (...)" »

In fact, the CNPD (in a truncated way) cites this recital 116 (in a truncated way) to justify its inaction in the face of a transfer of personal data beyond European borders.

Indeed, this recital does not establish an exception to the obligation to appoint a representative under Article 27 of the GDPR.

Secondly, recital 116 is in no way intended to relieve the national authorities of their responsibilities in relation to transfers of personal data to third countries. On the contrary, Recital 116 explains that the GDPR aims at seeking solutions to enable national data protection authorities to be more effective in such situations, in particular by promoting cooperation between national data protection supervisory authorities and by facilitating the establishment of international mutual assistance in this field. This recital thus concerns Article 50 of the GDPR, which specifically encourages the European Commission to implement cooperation agreements to facilitate the implementation of the GDPR. In any case, the absence of such agreements does not mean that such implementation should be abandoned as a matter of principle and that any complaint lodged by a controller without an establishment or representative in the EU should be rejected on the grounds that the CNPD and the other protection authorities would be incompetent to implement the GDPR.

On the contrary, the GDPR grants national data protection supervisory authorities extremely extensive and detailed powers, including investigative powers (Article 58 of the GDPR, to which Article 12 of the Act of ¹ August 2018 on the organisation of the CNPD refers) and

powers in terms of remedial measures (Articles 83 and 84 of the GDPR on administrative fines and sanctions and Section XI, entitled "Sanctions", of the Act of ¹ August 2018 on the organisation of the CNPD). It is precisely one of the major contributions of the GDPR to give national supervisory authorities "*a crucial role in ensuring compliance with the legal regime of data protection*" and in particular by accentuating their *law enforcement* role (E. DEGRAVE, "L'autorité de contrôle", in C. DE TERWANGNE and K. ROSIER (dir.), *Le règlement général sur la protection des données, Analyse approfondie*, Larcier p. 610 - see Exhibit 20. In the same sense, see R. ROBERT, "Les autorités de contrôle dans le nouveau règlement général sur la protection des données: statut, coopération et gouvernance européenne", in B. DOCQUIR (ed.), *Towards a European Data Protection Law*, pp. 21-24).

In particular, Article 83(4)(a), to which Article 48(1) of the Law of ¹ August 2018 on the organisation of the CNPD refers, provides that breaches of the "*obligations incumbent on the controller and the processor under Articles 8, 11, 25 to 39, 42 and 43*" (i.e., in particular, Article 27) are subject to "*administrative fines of up to EUR 10,000,000 or, in the case of an undertaking, up to 2% of its total annual worldwide turnover in the preceding financial year, whichever is the higher*". Thus, the GDPR gives the CNPD the mission and the means to sanction a violation of Article 27 such as the one committed by RocketReach.

It should be added that the possibility for national authorities to take measures whose scope goes beyond the territory of the European Union is nothing exceptional, since this possibility exists not only in the field of data protection but also in competition law, tax law and e-commerce: Thus, Directive 2000/31/EC on electronic commerce does not provide for "*any limitation, in particular territorial, on the scope of the measures which the Member States are entitled to adopt in accordance with this Directive*" and does not prevent injunctive measures "from having *global effects*", as the CJEU recently pointed out (CJEU, 3 October 2019, *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, pts. 49 and 50).

Moreover, it should be stressed that the CNPD has a very limited view of its concrete capacity for action when it states in the decision it has taken that "*it is impossible for it to ensure compliance with the provisions of the GDPR*" against a data controller established in the United States who has failed to *fulfil* its obligation to appoint a representative in the Union. Indeed, there are indeed possibilities to counter and sanction the practices of this data controller.

For example, article 50 of the law of ¹ August 2018 on the organisation of the CNPD provides that "*The recovery of fines or penalty payments is entrusted to the Administration of Registration and Domains. It is done as in the case of registration.*" Thus, if the CNPD pronounces a fine or penalty payment, it has at its disposal the significant means of the Luxembourg tax administration to enforce it. The Registration Administration can ensure the recovery of the sums due by resorting to a constraint procedure with regard to the company concerned or to a procedure of summons to a third party holder, not only on Luxembourg territory but also beyond by relying on the relevant instruments of Union law or even international law.

Another example is a cooperation protocol recently concluded between the Belgian Data Protection Authority and a non-profit association specialising in the registration of domain names: under this protocol, the association undertakes to block websites with the .be extension in application of the sanctions decided by the Authority. (Exhibit 21)

It follows that, faced with a manifest breach (and found by the CNPD itself) of a provision of the GDPR, such as Article 27, it is incumbent on the CNPD not only to investigate but also to take action to put an end to that breach, failing which it runs counter to the requirement of diligence set out in paragraphs 109 and 110 of the *Schrems II* judgment cited above.

In conclusion, the decision undertaken constitutes a violation by the CNPD of Article 57 of the GDPR and of its duty of care, and a violation of Articles 15 and 27 of the GDPR. The decision should therefore be reformed, if not annulled.

Noyb is still applying for a procedural allowance of 2,000 euros on the basis of Article 33 of the amended Act of 21 June 1999 on the Rules of Procedure before the Administrative Courts. It would indeed be unfair to leave all the costs not included in the costs, including the lawyer's fees, to be borne by him alone.

To these causes

The applicant, who is pre-qualified, claims that he should

Plea to the administrative court

Receive the present appeal in the form ;

Basically, to say it is justified ;

Going,

Mainly, reform the decision undertaken, annul the dismissal of the case, and :

- Order RocketReach to comply with article 27 of the GDPR,
- Order RocketReach to give effect to ██████████'s right of access on the basis of Article 15 GDPR,
- Order the CNPD to monitor the case and; if necessary, order a corrective measure in the sense of article 58 GDPR if RocketReach should not comply with the above injunctions;

In the alternative, reform the decision undertaken, annul the dismissal of the case, and refer the case back to the CNPD and order it to :

- Order RocketReach to comply with article 27 of the GDPR,
- Order RocketReach to give effect to ██████████'s right of access on the basis of Article 15 GDPR,
- Follow up the case for, failing or in case of impossibility to give effect to the right of access following the unlawful deletion of the data, pronounce a corrective measure within the meaning of Article 58 GDPR ;

In the further alternative, annul the decision taken and refer the case back to the CNPD;

Order the State of the Grand Duchy of Luxembourg to pay all the costs and expenses of the proceedings;

Order the State to pay the plaintiff a procedural compensation of 2,000 euros on the basis of article 33 of the amended law of 21 June 1999 on the rules of procedure before the administrative courts, even though it would be unfair to leave all the costs not included in the costs, including the lawyer's fees, to be paid by the State alone;

Give notice to the applicant that he reserves all other rights, means and actions;

Give notice to the applicant that it shall submit four copies of the following documents in support of its action:

- 1) Excerpt from the Austrian Register of Associations ("Vereinsregister")
- 2) Representation agreement
- 3) Copy of the decision taken
- 4) RocketReach home page
- 5) Exchange of emails of 5 April 2019
- 6) Claim
- 7) Exchange of emails of 9 April 2019
- 8) Email exchange (14 May 2019 and 11 July 2019)
- 9) Emails (three reminders and reply)
- 10) Email of 6 March 2020
- 11) Exchange of emails of 6 March 2020 and 17 March 2020
- 12) Emails of 28 March 2020, 19 April 2020, 26 April 2020
- 13) Letter from [REDACTED] 4 May 2020
- 14) Email of 25 May 2020
- 15) Email from [REDACTED] 29 May 2020
- 16) Email from the CNPD of 8 July 2020
- 17) Letter from [REDACTED] 10 August 2020
- 18) Statutes of the *noyb* association
- 19) GDPR Notice
- 20) E. DEGRAVE, "L'autorité de contrôle", in C. DE TERWANGNE and K. ROSIER (dir.), *Le règlement général sur la protection des données, Analyse approfondie*, Larcier
- 21) Cooperation protocol between DNS BELGIUM ASBL and the Belgian Data Protection Authority

Me Catherine WARIN

Luxembourg, 25 January 2021