APPEAL FOR REVERSAL

Before the administrative court

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

(decision of 16 October 2020)

Article 78 of the General Data Protection Regulation

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

The association under Austrian law *noyb - European Center for Digital Rights*, registered in the *Zentrales Vereinsregister under the* number 1354838270, domiciled 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, Agency 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 16 October 2020 (Exhibit 3).

IN FACT

The American company Zenleads Inc. operates under the name Apollo (Exhibit 4, company profile on the Bloomberg site). It summarises its services as follows on the home page of its website https://www.apollo.io (Exhibit 5, home page of the site): "*Use Apollo to find your ideal prospects and crack the code to convert them into customers*. "On its "*data*" page (Exhibit 6), it states: "*Find verified emails and direct dial phone numbers on 200 million contacts across 10 million companies, synced to your CRM*". The *pricing* page (Exhibit 7) also shows the rates for the company's various services. In other words, this company (based in the United States, more precisely at 535 Mission Street, San Francisco, CA according to the information available on its website) collects and markets personal data, including data of European Union residents, to enable its customers to identify potential customers themselves.

In August 2020, [redacted] established that Zenleads had collected certain personal data concerning him, made a request for information on the processing of his data in accordance with Article 15 (1) of the GDPR via the option "*Request Access to Collected Data*" available on the "*privacy"* page of the Apollo website (Exhibit 8).

On 13 June 2020, Apollo responds to [redacted] (Exhibit 9). It explained that before exercising its right of access, [redacted] should complete an *Identity Verification Form* (Exhibit 10). According to Apollo, "*this is important, to avoid providing personal information to someone 'spoofing' an identity*".

On 8 July 2020, [redacted] sent a claim to the CNPD (Exhibit 11, claim), noting that Apollo had not complied with its request.

On the same day, the CNPD acknowledges receipt of the complaint of [redacted] (Exhibit 12, acknowledgement of receipt).

On 28 July 2020, the CNPD asked [redacted] for additional information regarding its claim (Exhibit 13, email).

[redacted] replies by two emails dated 28 July 2020 and [1] August 2020 (Exhibit 14).

By email dated 13 August 2020 (Exhibit 15), the CNPD informs [redacted] that a first examination of its claim "*has confirmed that the controller is located in the United States of America*". It continues as follows: "*although we can communicate with the data controller, we do not have the powers to investigate and enforce any decisions we may take in the United States of America.*

We therefore inform you that we are dealing with your complaint with a view to cooperation from the controller, given that we do not have the power to impose actions on the controller to improve its data protection practices, with the consequence that it would be impossible for us to pursue your complaint effectively in the absence of cooperation from the controller. »

In two emails dated 13 August 2020 and 23 August 2020, [redacted] appropriateness of the limits that the CNPD imposes on its own competences (Exhibit 16).

On 16 October 2020, the CNPD sends to [redacted] decision undertaken, which reads as follows :

[redacted],

The (CNPD) goes back to your complaint of 8 July 2020 relating to your request for access to your personal data processed by the "apollo.io" site.

As indicated in our previous letter dated 18 September 2020, the CNPD has contacted the data controller in order to try to resolve the problem raised by your complaint, in this case the sending of an automated form in response to your access request.

We would like to inform you that this contact has unfortunately remained unanswered.

We therefore regret to inform you that, subject to a possible subsequent return by the controller of which we would keep you informed, we consider that it is impossible for us to effectively pursue the processing of your complaint.

Indeed, as already mentioned in our previous responses of 13 July and 18 September 2020, the CNPD has no means of action against a data controller established on the territory of the United States of America which does not have an establishment on the territory of the European Union (EU) or which has not designated a representative in the EU under Article 27 of the GDPR. Indeed, in these cases, it is impossible for it to enforce the provisions of the GDPR on the territory of the United States of America.

(...) »

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 General Data Protection Regulation (Regulation 2016/679 of 27 April 2016, hereinafter "GDPR") entitled "***Representation of*** data ***subjects*****"** 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.*

The plaintiff, having already brought several proceedings in different Member States on the basis of this provision, fulfils all these criteria, as can be seen from its statutes (Exhibit 17):

- it is a non-profit-making association (§2 of the statutes (Exhibit 17): "*Der Verein, dessen Tätigkeit nicht auf Gewinn gerichtet ist...")*
- the association, which has its seat in Vienna, is governed by Austrian law (§1(4) of the statute and Exhibit 1)
- its statutory objectives are of public interest and the association acts in the field of the protection of personal data : " *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 (CNPD) provides: "*An appeal against the decisions of the CNPD taken pursuant to this Act shall be lodged with the Administrative Court, which shall rule as judge of the merits.* "Furthermore, the CNPD Regulation entitled "*Procedure for claims before the CNPD*" takes good account of these requirements since it contains 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 these 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 (...)* ***bring an appeal for reversal before the administrative court within 3 months of 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, the 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 the Tribunal 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

In its email of 13 August 2020 (Exhibit 15), the CNPD warned [redacted] that in the absence of the "*collaboration*" of the US-based controller, it would be impossible for it to continue processing the claim. The decision taken on 16 October 2020 (Exhibit 3) confirms that, as Apollo "*unfortunately" did* not follow up on the CNPD's attempt to contact it, the CNPD considers that it is "impossible for it to *effectively pursue*" the processing of [redacted]s claim.

Thus, the CNPD announces that "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 United States of America who does not have an establishment on the territory of the European Union (EU) or who has not appointed a representative in the EU pursuant to Article 27 of the GDPR. Indeed, in these cases, it is impossible for it 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 silence of the company concerned to the CNPD's requests is therefore insufficient to justify the CNPD's 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.

Precisely, in the present case, the explanations provided by the CNPD merely highlight the unlawfulness of its decision in the light of 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.

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 this case, Zenleads offers its clients: "*Use Apollo to find your ideal prospects and crack the code to convert them into* customers. "On its "*data*" page (Exhibit 6), it states: "*Find verified emails and direct dial phone numbers on 200 million contacts across 10 million companies, synced to your CRM*". Thus, this company collects and markets personal data, in particular data relating to the professional activity of European Union residents, to enable its customers to identify potential customers themselves. This data processing therefore falls within the scope of the GDPR.

Zenleads itself acknowledges the applicability of the GDPR to its business, as indicated in the "*data privacy bot"* for visitors to its website (Exhibit 18, screenshot and enlargement): "*Under the EU General Data Protection Regulation, we need your approval for our use of personal information (e.g. your name and email address) you may provide as we communicate (...)".*

Therefore, there is no doubt as to the applicability of the provisions of the GDPR to the present case.

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

By finding that Zenleads, a US-based company, has not "*designated 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 Apollo's equally clear violation of at least one other provision of the GDPR, namely Article 15, which establishes 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 remembered that when [redacted] sought to assert the rights protected by that provision, Apollo merely replied by returning an automated form requesting additional information (Exhibit 10), assuming that [redacted] had requested a copy of its data, which was not the case. Indeed, [redacted] exercise its right to obtain a copy of the data (Article 15(3) GDPR): it only requested information about the data processing of which it was the subject, as permitted by Article 15(1) of the GDPR. Apollo therefore wrongly requested more information to identify [redacted] and to provide him with "personal information". Indeed, it is entirely possible to provide the information provided for in article 15 (1) of the GDPR without requiring proof of identity from the person concerned. Such a request for additional information is moreover likely to contravene Article 11 of the GDPR, which provides precisely for this case. At the very least, it was also incumbent on the CNPD to investigate this violation of the rights of [redacted].

E. The failure of the CNPD to meet its obligations

Having found that Apollo, a company established in the United States, had not appointed a representative as required by Article 27 of the GDPR, the CNPD concluded that it did 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 indicates that it tried to contact the Apollo company. However, in view of the latter's lack of response and the absence of a designated representative on Union territory, the CNPD decided to discontinue processing the case.

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 its position, the CNPD quotes in its email of 13 August 2020 (Exhibit 15) 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 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 broad 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 19. 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 Apollo.

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 non-profit association undertakes to block websites with the . be extension in application of sanction decisions taken by the Authority (exhibit 20).

It follows that, faced with a manifest breach (and recognised by the CNPD) of provisions of the GDPR such as Articles 27 and 15, 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 would run 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 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

Complaint 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 Apollo to comply with article 27 of the GDPR,

- Order Apollo to give effect to [redacted]'s right of access on the basis of article 15 GDPR,
- Order the CNPD to monitor the case and, if necessary, if Apollo fails to comply with the above injunctions, to order a corrective measure within the meaning of Article 58 GDPR;

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 Apollo to comply with article 27 of the GDPR,
- Order Apollo to give effect to [redacted]'s right of access on the basis of article 15 GDPR,
- Monitor the case and, in the event that Apollo fails to comply with the injunctions given, issue a corrective measure in the sense 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) Zenleads company profile on the Bloomberg website
5) Home page of the apollo.io website
6) Page " *data*
7) Page " *pricing* "
8) Page " *privacy* "
9) email of 13 June 2020
10) *Identity Verification Form*
11) Claim of 8 July 2020
12) Acknowledgement of receipt
13) Email of 28 July 2020
14) Emails of 28 July 2020 and [1] August 2020
15) Email of 13 August 2020
16) Emails of 13 August 2020 and 23 August 2020
17) Statutes of the *noyb* association
18) Screenshot and enlargement of the "*data privacy bot*" message
19) 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

20) Cooperation protocol between DNS BELGIUM ASBL and the Belgian Data Protection Authority

Me Catherine WARIN

Luxembourg, 25 January 2021