



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

SECOND SECTION

CASE OF UAB AMBERCORE DC AND UAB ARCUS NOVUS v. LITHUANIA

(Application no. 56774/18)

JUDGMENT

Art 6 § 1 (civil) • Administrative proceedings concerning refusal on national security grounds to issue applicant companies with permit to build data centre • Refusal based only partly on non-disclosed classified information of no apparent decisive value • Applicant companies given opportunity to effectively participate in proceedings • Due exercise by administrative courts of powers of scrutiny, giving reasons for decisions with regard to specific case-circumstances • Restrictions on rights to adversarial proceedings and equality of arms offset in such a manner that fair balance between parties not affected to such an extent as to impair very essence of right to a fair hearing

STRASBOURG

13 June 2023

FINAL

13/09/2023

*This judgment has become final under Article 44 § 2 of the Convention.
It may be subject to editorial revision.*

In the case of UAB AmberCore DC and UAB Arcus Novus v. Lithuania,

The European Court of Human Rights (Second Section), sitting as a Chamber composed of:

Arnfinn Bårdsen, *President*,

Jovan Ilievski,

Egidijus Kūris,

Saadet Yüksel,

Lorraine Schembri Orland,

Frédéric Krenç,

Davor Derenčinović, *judges*,

and Dorothee von Arnim, *Deputy Section Registrar*,

Having regard to:

the application (no. 56774/18) against the Republic of Lithuania lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by two companies registered in Lithuania, UAB AmberCore DC (“the first applicant company”) and UAB Arcus Novus (“the second applicant company”), on 28 November 2018;

the decision to give notice to the Lithuanian Government (“the Government”) of the complaints concerning the applicant companies’ right to a fair hearing and right to protection of property;

the parties’ observations;

Having deliberated in private on 9 May 2023,

Delivers the following judgment, which was adopted on that date:

INTRODUCTION

1. The case concerns the applicant companies’ complaint, under Article 6 § 1 of the Convention, that they did not have a fair hearing during administrative court proceedings in which administrative decisions refusing them permission to build a data centre were upheld. Under Article 1 of Protocol No. 1 to the Convention, the applicant companies further complained that they had incurred losses because they had not received security clearance to build the data centre.

THE FACTS

2. The applicant companies, AmberCore DC and Arcus Novus, are registered at a technology park in Liepiškės near Vilnius. They were represented before the Court by Mr R. Simaitis, a lawyer practising in Vilnius.

3. The Government were represented by their Agent, Ms K. Bubnytė-Širmenė.

4. The facts of the case, as submitted by the parties, may be summarised as follows.

5. According to information on the applicant companies' websites, Arcus Novus was founded in 2003 and deals with the implementation and development of technological projects, including the transmission of information by satellite telecommunication. In 2009 Arcus Novus established a subsidiary company, later renamed AmberCore DC, which deals with the construction and development of data centres. The companies note that AmberCore DC is owned by a group of private investors and has experience in telecommunications and the operation of high-tech telecommunication facilities.

I. FIRST SET OF ADMINISTRATIVE PROCEEDINGS

6. It appears from the documents submitted by the parties that in February 2015 Arcus Novus, as the sole shareholder of AmberCore DC, increased the share capital of the latter and acquired all its shares.

7. On an unknown date, the applicant companies initiated a project to build a data storage facility near Vilnius.

In July 2016 Arcus Novus asked the Lithuanian authorities to assess its compliance with the interests of national security, as required by Article 7 §§ 10 (3) and (4) of the Law on Enterprises and Facilities of Strategic Importance to National Security and Other Enterprises of Importance to Ensuring National Security (hereinafter "the Law on Enterprises and Facilities of Strategic Importance", see paragraph 70 below).

8. On 11 July 2016 the Chancellery of the Government (hereinafter "the Chancellery") asked Arcus Novus to submit the necessary information about the company and its activities. On 19 July 2016 Arcus Novus submitted the necessary documents.

9. On 19 July 2016 the Chancellery inquired with a number of Lithuanian institutions regarding Arcus Novus's compliance with national security interests.

A. The Commission's protocol decision no. NS-23 of 16 August 2016 and related administrative court proceedings (administrative case no. eA-3729-415/2018)

10. By protocol decision (*protokolinis sprendimas*) no. NS-23 of 16 August 2016, the Commission for Assessment of Compliance of Potential Participants with National Security Interests (*Potencialių dalyvių atitikties nacionalinio saugumo interesams įvertinimo komisija* – hereinafter "the Commission") unanimously held that Arcus Novus did not comply with the conditions set out in Article 7 §§ 10 (3) and (4) of the Law on Enterprises and Facilities of Strategic Importance (see paragraph 70 below). The

Commission's decision was based on report no. 19-1379 of 5 August 2016 issued by the State Security Department (hereinafter "the SSD"). On the basis of that report the Commission held that Arcus Novus, through intermediary companies, including SatGate Holding ApS and SatGate Investments Ltd., which were registered abroad in Denmark and Malaysia, was owned and controlled by four citizens of the Russian Federation, K.L., V.A., V.M. and B.M. The risk posed by Arcus Novus to Lithuanian national security was increased by the fact that one of these owners, V.A., had previously worked in Russian companies directly linked with the Russian State and law-enforcement authorities. Those companies "were overseen" (*ju veiklą prižiūri*) by the Federal Security Service of the Russian Federation ("the FSB"). More specifically, from 2006 to 2009 V.A. had worked as a director of the Russian gas corporation's subsidiary company Gazprom Komplektacija in the Kaliningrad region, and from 2009 to 2014 had been the founder and deputy director of Gazinvest Group, another company operating in Kaliningrad and dealing in customs brokerage. In Lithuania, the data storage facility was to be connected to the Internet and the Lithuanian telecommunications networks, and, through them, to the member States of the European Union (EU) and the Russian Federation. It was likely that when the data storage facility was connected to Russia, it would be connected to the FSB's Radio-Electronic Intelligence Centre, which carried out radio electronic intelligence activities and cyber spying against Lithuania and other North Atlantic Treaty Organisation (NATO) and EU member States. "According to the assessment by the SSD" (*VSD vertinimu*): (i) the FSB would then be able to intercept the data stored at the facility by Lithuanian and foreign State institutions, companies and organisations and thus gather intelligence; (ii) the FSB would be able to impact the Lithuanian telecommunications networks; (iii) Lithuanian territory could be used to carry out cyberattacks against third countries; and (iv) if [Lithuanian] State institutions, commercial banks and telecommunications companies became clients of the data storage facility, Russia could disrupt the functioning of the Lithuanian State and its economy.

11. The Commission also held that Arcus Novus, when increasing the share capital of AmberCore DC and acquiring its shares in February 2015 (see paragraph 6 above), had failed to ask the Commission to assess Arcus Novus's compliance with national security interests, thus breaching Article 7 § 2 (2) of the Law on Enterprises and Facilities of Strategic Importance.

The Commission's decision also read that "information on Arcus Novus's compliance with the interests of national security should be provided to Arcus Novus".

12. On 18 August 2016 the applicant companies were sent a letter by the Chancellery (*raštas*) no. S-72-2767) regarding the results of the screening as to their compliance with national security interests.

B. Proceedings before the Vilnius Regional Administrative Court

13. The applicant companies contested the Commission's protocol decision in administrative court. They argued, among other things, that the protocol decision lacked any factual basis and restricted their legitimate interests since it barred them from pursuing the data centre project. They also argued that no documents other than the Commission's protocol decision no. NS-23 and the Chancellery's letter no. S-72-2767 had been provided to them. They asseverated that they had no intention of linking the data centre via the Internet to the Radio-Electronic Intelligence Centre in the Russian Federation. They also denied that their shareholder V.A. had links to the Russian security services.

14. The Commission replied that its findings had been based on the information referred to in the protocol decision, as well as the SSD's "classified" (*slaptai*) report no. 19-1379 of 5 August 2016, which supplemented the unclassified factual information that had led to the decision. The Commission considered that the court could find its decision justified even without classified information, solely on the basis of the explanations it had given.

15. The SSD, which had the status of an interested third party in the proceedings, pointed out that the applicant companies, when seeking to attract potential clients to implement the project and inviting the Lithuanian State institutions to make use of their services, had openly named as their partner the Russian concern Gazprom, which had close links to the Russian special services. The applicant companies' statements that the protocol decision was not based on any objective information (facts), arguments or evidence did not correspond to reality and were misleading. Furthermore, the applicant companies, when presenting the data centre project, had specified that when implementing it, data transfer infrastructure would be developed internationally so that the data centre would be linked to Europe, Scandinavia and Russia. This information was supported by the data centre project presentation material.

16. According to the Government's observations of 19 November 2020, at that stage of the administrative court proceedings, the parties provided the Vilnius Regional Administrative Court with the documents described below.

17. On 13 January 2017 the Chancellery, together with its response to the applicant companies' complaint, provided material not containing information constituting a State secret, including: various documents about the applicant companies' shareholder structure; a number of documents from the Lithuanian authorities, including a copy of the Commission's protocol decision no. NS-23 of 16 August 2016; a copy of a letter of 16 August 2016 by the SSD to the Government Chancellor (*kancleriui*) stating that the intended project posed a threat to national security given that its developers intended to link the data centre via fibre-optic cables to the FSB's

Radio-Electronic Intelligence Centre in Russia; and copies of replies from the Lithuanian law-enforcement authorities on whether they had any kind of information about the applicant companies relevant for their assessment regarding their possible threat to national security.

18. For its part, on 13 February 2017 the SSD provided the court of first instance with AmberCore DC's presentation of the data storage facility project, together with its response to the applicant companies' complaint.

19. On 13 February 2017, complying with a ruling by the Vilnius Regional Administrative Court of 12 January 2017, the Chancellery provided that court with nineteen pages of classified information related to the applicant companies' complaint regarding the Commission's protocol decision of 16 August 2016.

20. On 28 February 2017 the applicant companies asked the court to hear the case in public and not to add classified documents to the case file.

21. According to the Government's observations, following a request by the applicant companies on 28 February 2017, the Vilnius Regional Administrative Court twice asked the SSD, on 23 March and 3 April 2017, to declassify the classified documents submitted in the administrative case on 17 February 2017 (the SSD's letter no. 19-223). On 25 April 2017 the court received a response from the SSD stating that since the time frame for the duration of classification had not yet expired and the need for classification remained, the documents could not be declassified.

22. According to the Government's observations, on 8 May and 28 June 2017 the applicant companies also asked the Vilnius Regional Administrative Court to adjourn the hearings owing to their inability to participate, requests which were both granted by the court of first instance. During a hearing on 27 September 2017, the applicant companies submitted a request to adjourn the case in order to reach a settlement with the Commission, which was granted by the court of first instance. During a hearing on 6 December 2017, the applicant companies submitted a request to examine two witnesses, V.A. and V.M., which was granted by the court of first instance, and the persons indicated in the Commission's decision under appeal as persons whose relations caused a risk to the national security of Lithuania were examined as witnesses. At the same hearing, the applicant companies submitted a request asking for certain classified material not to be recognised as evidence in the case, but it was refused by the court of first instance.

23. The Vilnius Regional Administrative Court decided the case in non-public oral proceedings, in which the applicant companies' representatives K.L. and V.T., their lawyers, and representatives of the Chancellery, the Commission and the SSD took part.

24. On 16 January 2018 the applicant companies' complaint was dismissed as unfounded. The court noted that the dispute between them and the Commission no longer existed, because on 19 April 2017 a court-approved settlement agreement had been signed pursuant to which the

agreement to increase the share capital (see paragraph 6 above) had been invalidated.

The court also held that if the applicant companies considered that the Commission's protocol decision had damaged their business reputation, they could defend that in civil proceedings.

25. The applicant companies appealed.

C. Proceedings before the Supreme Administrative Court

26. In its response to the applicant companies' appeal, the SSD observed that the first-instance court had not examined and assessed the classified documents that the SSD had provided to it, which had been relevant for the Commission when adopting the protocol decision. The SSD stated that, if the Supreme Administrative Court decided to assess all the circumstances that had led to the adoption of the protocol decision and all the arguments by the applicant companies, the SSD would provide it with those documents, which had already been provided to the Commission and the first-instance court.

27. On 26 March 2018 the applicant companies requested that the case be examined under the urgent procedure, on the grounds that due to the ongoing litigation they had been incurring serious losses. The request was granted by the Supreme Administrative Court two weeks later, on 4 April 2018.

28. By a ruling of 30 May 2018, the Supreme Administrative Court observed that the Commission's protocol decision no. NS-23 of 16 August 2016 (see paragraphs 10 and 11 above) "was based, among other things, on classified documents (*įslaptinti dokumentai*)" provided by the SSD to the Commission, and that those documents formed the factual basis for the protocol decision. The Supreme Administrative Court stated that "[to date] the classified material [had] not been included in the case file [before it], and [that it was] necessary in order to assess whether the Commission's protocol decision was lawful and reasoned". The Supreme Administrative Court thus ordered the SSD to provide those documents to it.

29. It appears from the material in the case file that afterwards, on 6 June 2018, the Prosecutor General's Office informed the Supreme Administrative Court that its judges could consult the classified information at its premises, which had secure facilities for such a purpose. On 11 June 2018 the Supreme Administrative Court thus informed the SSD that the judges would consult the classified information at the premises of the Prosecutor General's Office.

30. On 27 June 2018 the Supreme Administrative Court examined the case in written proceedings and left the first-instance court's decision unchanged. It referred to, among other things, Article 2 §§ 1 and 2, Article 3 § 3 (3) and Article 7 of the Law on Enterprises and Facilities of Strategic Importance as regards national security interests and the telecommunications sector (see paragraph 70 below). Regarding the applicant companies' compliance with the interests of national security, the

court held that the information indicated in protocol decision no. NS-23 (see paragraph 10 above), examined and assessed by the first-instance court, constituted the factual basis for finding that Arcus Novus had links with the FSB, those links posing a threat to Lithuania's national security. Accordingly, there was no legal basis for finding that the applicant company met the national security requirements, within the meaning of Article 7 § 10 (3) and (4) of the Law on Enterprises and Facilities of Strategic Importance. In the words of the court, "that information [was] not contradicted by the classified documents examined by the appellate court".

31. The Supreme Administrative Court also referred to Article 46 of the Constitution (see paragraph 69 below) and the Constitutional Court's case-law to the effect that that provision was inseparable from such constitutional values as State independence and territorial integrity. In the context of the case at hand, it was relevant that legal measures taken to protect the information technology and telecommunications sector, which was of strategic importance to national security, from possible external impact from countries unfavourable to the State of Lithuania in terms of their geopolitical orientation, or from the individuals closely linked to those States, were inseparable from the State's obligation set out in Article 46 § 3 of the Constitution to regulate economic activity so that it served the general welfare of the nation and did not breach the constitutional principle of proportionality.

32. In response to the applicant companies' grievance of discrimination (on the basis of nationality), the Supreme Administrative Court observed that the principle of non-discrimination did not negate the possibility of different legal regulation being established for certain categories of persons in different situations. As pointed out by the Constitutional Court, the constitutional principle of equality did not negate the possibility of treating persons differently according to their status (see paragraph 74 below). Accordingly, national security guarantees constituted a constitutionally justifiable ground for restricting persons' activity in economic sectors of strategic importance. Besides, Article 8 § 3 of the Law on Investments (see paragraph 71 below) also provided that investment in sectors of important for national security interests was only allowed after having assessed the compliance of a potential participant.

33. The Supreme Administrative Court thus found that the contested individual administrative decision – the Commission's protocol decision – was based on objective evidence (facts), had a basis in law and was reasoned.

II. SECOND SET OF ADMINISTRATIVE PROCEEDINGS

A. The Commission's protocol decision no. NS-49 of 24 November 2017 and related administrative court proceedings (administrative case no. eA-4143-442/2018)

34. On 11 October 2017 the two applicant companies and SatGate Holding ApS (see paragraph 10 above) asked the Commission to verify, under Article 7 § 2 (2) of the Law on Enterprises and Facilities of Strategic Importance, SatGate Holding ApS and Arcus Novus's compliance with the interests of national security. The companies intended to conclude a business transaction so that SatGate Holding ApS would obtain 100% of Arcus Novus's shares. Given that the latter company already controlled 100% of AmberCore DC's shares, SatGate Holding ApS would obtain control over the company AmberCore DC, which operated in the sector of information technology, telecommunications and other high technology of strategic importance to national security.

35. On 16 October 2017 the Commission wrote to the Ministry of Foreign Affairs, the Ministry of the Interior, the Prosecutor General's Office, the SSD, the Financial Crimes Investigation Service, the Police Department and the Special Investigation Service, asking for their conclusions regarding the two companies' compliance with the interests of national security.

36. On 6 November 2017 the Commission held that it did not have sufficient information about the shareholders of SatGate Holding ApS, and that the information in its possession was "contradictory or [had not been] fully disclosed". Three days later the Commission asked the companies to provide information regarding what companies were owned by the SatGate Holding ApS shareholders K.L., V.T., V.M., M.G. and V.A., as well as to provide information about several other linked companies. Representatives of SatGate Holding ApS, Arcus Novus and AmberCore ApS provided that information to the Commission on 16 November 2017.

B. The Commission's protocol decision no. NS-49

37. On 24 November 2017 the Commission unanimously adopted a second protocol decision, no. NS-49, holding that Arcus Novus and SatGate Holding ApS did not meet the requirements of Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance. On the basis of information received from the applicant companies' lawyers, the Commission concluded that Arcus Novus was controlled, through intermediary companies registered abroad, by Russian citizens K.L., V.M. and V.A., the latter having been a shareholder of several other companies registered in Lithuania, New Zealand and the Russian Federation.

38. The Commission also held that, according to the assessment by the SSD, SatGate Holding ApS and Arcus Novus had links to the Russian FSB, which posed a threat to the national security of Lithuania. The circumstances established in the report regarding Arcus Novus's non-compliance with the requirements of Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance, which the SSD had provided to the Commission in 2016 (see paragraph 10 above), related to V.A., remained unchanged. Even if V.A. were to sell his shares in Arcus Novus to SatGate Holding ApS, he would retain influence in Arcus Novus.

39. The Commission also noted that "when examining the question regarding [Arcus Novus's] compliance with the interests of national security, not only public but also declassified (*išslaptinta*) information provided by competent institutions [had been] assessed".

40. The applicant companies appealed against the Commission's protocol decision, as did SatGate Holding ApS.

C. Proceedings before the Vilnius Regional Administrative Court

41. According to the Government's observations of 19 November 2020, during this (second) set of administrative court proceedings, the following unclassified documents were provided by the parties to the Vilnius Regional Administrative Court.

42. On 28 December 2017 the applicant companies provided that court with material including, among other things, various documents regarding the applicant companies' shareholder structure and internal regulations. The material also included copies of the following: the Commission's protocol decision no. NS-23 of 16 August 2016 (see paragraph 10 above); the Chancellery's letter of 18 August 2016 to Arcus Novus stating that it did not comply with the national security interests criteria (see paragraph 12 above); the Commission's protocol decision no. NS-49 of 24 November 2017 (notified to the applicant companies' lawyers by the Commission on 1 December 2017, see paragraphs 37-39 above); a copy of the Chancellery's request to the applicant companies' lawyers for additional information regarding the direct and indirect shareholders of SatGate Holding ApS, and the applicant companies' lawyers' reply to that request, together with that additional information (see paragraph 36 above).

43. On 3 January 2018 the Chancellery, together with its response to the applicant companies' appeal, provided the first-instance court with material relating to the dispute, which did not contain information constituting a State secret and included the above-mentioned decisions of the Commission and various documents about the applicant companies' shareholder structure and internal regulations. It also contained a copy of an email of 2 November 2017 sent by the Ministry of Foreign Affairs to the Commission indicating that, on the basis of information from the UK companies registers, they "presumed"

(*darome prielaidą*) that V.A., whom the SSD had seen as having connections making him a threat to national security, could remain in the AmberCore DC project and remain its developer, which would mean that the threat to national security would persist.

44. On 26 January 2018 the SSD, as an interested third party in the proceedings, provided the Vilnius Regional Administrative Court with a six-page long response to the applicant companies' complaint. The response gave a detailed account of the threat posed by the applicant companies to the interests of national security, on account of, among other things, the companies' shareholders and ownership structure, and the past links of one of its owners, V.A., to Gazprom (see paragraphs 49 and 50 below). The SSD also provided the court with a copy of the "Project presentation leaflet on the data storage facility by AmberCore DC", in which Gazprom had been mentioned among the "partners" or "customers" of the SatGate Group of companies.

45. The case was heard by the Vilnius Regional Administrative Court in closed hearings, with the participation of both applicant companies' representatives and lawyers. At the applicant companies' request, V.A. and V.M. (see paragraph 37 above) were examined as witnesses.

46. The applicant companies acknowledged that on 1 December 2017 they had received a letter from the Chancellery (*raštas*) no. S-3315 enclosing an extract (*išrašas*) of the Commission's protocol decision no. NS-49 of 24 November 2017 (see paragraphs 37-39 and 42 above). The applicant companies nevertheless claimed that the protocol decision had no factual basis and unjustifiably restricted their rights and lawful interests. They also pleaded that they had already invested in the data centre project, and that entities (*subjektai*) from Russia and Denmark had already invested. The negative assessment by the Commission made it impossible to continue developing the project and would deprive the investors of the "large sums of money already invested".

47. The applicant companies also contested the Commission's finding that Arcus Novus was controlled, via intermediary companies registered abroad, by Russian citizens K.L., V.M. and V.A. They also argued that "presumptions" (*prielaidos*) in the protocol decision regarding V.A. and his Russia-related links (see paragraph 10 above) could not be the basis for finding that a person did not comply with national security interests. As argued by the applicant companies, "having acquainted themselves with the protocol decision, they had asked V.A. to clarify the real situation. V.A. had explained that the circumstances referred to by the Commission did not correspond to reality, as he had never worked or otherwise been linked to intelligence organisations in Russia or any activities which would be hostile to the interests of the Republic of Lithuania". The applicant companies considered that the Commission's decision was in breach of the principle of non-discrimination.

48. On 8 March 2018 the Vilnius Regional Administrative Court dismissed the applicant companies' appeal regarding the Commission's protocol decision no. NS-49 of 24 November 2017.

49. The court noted that it appeared from the content of the protocol decision of 24 November 2017 that the Commission, based on the assessment by the SSD, had established that SatGate Holding ApS and Arcus Novus had links with the FSB of the Russian Federation, conducting intelligence operations against Lithuania, which posed a risk to national security, and that therefore they did not meet the requirements of Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance, given that the information provided suggested the applicant companies had links with foreign special services. In the protocol decision, the Commission had established that the risk to Lithuania's national security had increased due to the fact that V.A. had previously worked in Russian companies directly linked to the Russian government and law-enforcement authorities (see paragraph 10 above).

50. The court further noted that the applicant companies disagreed with the Commission's assessment and maintained that its arguments regarding V.A.'s connections had no factual basis. However, the court stated that the Commission had reached its decision on the basis of the SSD's material (both publicly available and classified) that V.A. had connections with Gazprom Komplektacija in Kaliningrad and with Gazinvest Group. The Law on Enterprises and Facilities of Strategic Importance did not specify which relations should be considered a threat to national security and which existing relations caused a person to be recognised as not complying with the requirements of Article 7 § 10 (4) of that Law. Referring to established case-law of the Supreme Administrative Court (ruling of 11 August 2016 in case no. A-4560-662/2016, and ruling of 13 October 2017 in case no. A-5137-624/2017), the Vilnius Regional Administrative Court pointed out that State security was an essential element (*valstybės saugumas yra esminę reikšmę turinti aplinkybė*), important for all members of society; it was a fundamental value (*pagrindinė vertybė*) which took priority over possible violations of individual rights. A threat to national security was a circumstance considered important when deciding on the State's national interests. A threat to national security could also occur as a potential threat (the Supreme Administrative Court's ruling of 23 June 2010 in case no. A858-1810/2010). The Commission had discretion to assess whether specific persons could be considered to pose a real or potential threat to national security. The Commission had to exercise its discretion on the basis of objective information, namely that received from the entities specified in Article 7 § 6 of the Law on Enterprises and Facilities of Strategic Importance, which were assigned the function of collecting operational material to ensure the State's security. Besides, the Commission's discretion had to be exercised in the light of the principles of objectivity, impartiality, lawfulness and proportionality.

51. The Vilnius Regional Administrative Court then referred to the information “provided in the case by the SSD” from which it was apparent that the data centre project posed a threat to Lithuania’s national security because of its founders’ intent to link it to Russia (the court referred to the information set out in paragraph 10 above). The court also noted that the data centre project was a private initiative, which aimed to provide information technology and telecommunications services in the data centre. Until the project was implemented, the list of persons/subjects (*subjektų ratas*) who would use those services would not be defined. However, from the project presentation leaflet submitted, it was evident that the project was intended to contribute to the development of strategic infrastructure related to the State’s national security, and that data would be transmitted across State borders, including to Russia. In such circumstances, the court concluded that “the information in the case file confirmed” that when implementing the project, data which could be linked to State security would be stored in the centre, the protection of which formed part of the guaranteeing of State security. Taking that into account, the possibility of other States’ security services taking part in the project through interested persons clearly amounted to a danger to State security. It was worth pointing out that publicly accessible (*viešai prieinama*) information confirmed the circumstances established by the Commission regarding V.A.’s links to the Russian company Gazprom, which was overseen by the Russian FSB. The court also noted that from 2006 to 2009 V.A. had been the director of Gazprom’s subsidiary company in Kaliningrad (see paragraph 10 above). Those circumstances had not, for the most part, been contested by the applicant companies and SatGate Holding ApS.

52. In the light of the above, the court found it established that Arcus Novus and SatGate Holding ApS, which (both) had direct links with V.A., posed a threat to national security because of the latter’s links to the Russian security and intelligence services. Having regard to the above, the court held that the Commission had lawfully and reasonably acknowledged that Arcus Novus and SatGate Holding ApS did not meet the requirements of Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance. The applicant companies’ arguments that they had already invested in the data centre project had had no impact on the Commission’s decision.

53. The court also noted that one of the applicant companies’ main grievances was that the Commission’s decision was essentially based on information classified under the rules established by law, and that they had had no possibility of seeing that information. They argued that classified evidence was inadmissible because it restricted their right to a defence.

54. As to evidence, the court referred to Article 56 § 3 of the Law on Administrative Proceedings, pursuant to which factual information constituting State or official secrets “as a rule” (*paprastai*) could not constitute evidence in administrative proceedings, until it was declassified (see paragraph 73 below). However, according to the Supreme

Administrative Court's practice, "as a rule" meant that in certain situations classified information could be considered admissible evidence, which could be assessed by the court under the rules set out in Article 56 § 6 of the Law on Administrative Proceedings. This was in a situation where it was not the only evidence, proving or disproving circumstances important for the case, and where the unclassified evidence in the case was reliable and sufficient to substantiate established factual circumstances (the Supreme Administrative Court's ruling of 28 October 2014 in case no. A143-1456/2014). As noted by the Supreme Administrative Court, such an explanation essentially also corresponded to the Constitutional Court's position in the ruling of 15 May 2007 (see paragraph 75 below) and the Court's case-law under Article 6 § 1 of the Convention (the Supreme Administrative Court referred to *Meral v. Turkey*, no. 33446/02, 27 November 2007; *Miran v. Turkey*, no. 43980/04, 21 April 2009; *Topal v. Turkey*, no. 3055/04, 21 April 2009; and *Gulijev v. Lithuania*, no. 10425/03, 16 December 2008).

55. In the case at hand, the protocol decision was not based on exclusively classified information which the applicant companies had been unable to access. The court noted that "publicly available information and the unclassified information by the SSD and the Commission [had been] sufficient to adopt the contested protocol decision, that is, to hold that the applicant companies did not meet the requirements of Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance". The court had no basis for doubting the objectivity and reliability of the unclassified documents provided by the SSD, and, moreover, that those documents were supported by classified documents provided by the SSD, which the court had also assessed. In the light of the foregoing, the court held that the applicant companies' right to have their rights defended in court (*teisė į teismo gynybą*) had not been breached. Likewise, there was no reason to declare the classified information provided by the SSD as inadmissible evidence. When the protocol decision had been adopted, the reality of the possible threat to State security (*galimos grėsmės valstybės saugumui realumas*), which in this case had been objective and proven on the basis of the information referred to in the protocol decision and in the SSD's reports, had been assessed.

56. Lastly, because of the content and nature of classified information, which was linked to State security interests, not all the arguments leading to the adoption of the protocol decision could have been disclosed in the protocol decision. However, this was not a reason to acknowledge that the protocol decision lacked basis. The applicant companies' right to a defence in court had not been breached. The protocol decision met the essential requirements of an individual administrative decision – it contained a factual basis and a legal assessment had also been provided. It followed that the protocol decision was lawful and reasoned.

D. Proceedings before the Supreme Administrative Court

57. The applicant companies lodged an appeal with the Supreme Administrative Court, arguing that the first-instance court had merely restated in its reasoning what had been said in the Commission’s decision and had failed to evaluate any of the circumstances to assess its reasonableness. Moreover, the first-instance court had also failed to properly examine the evidence submitted. It had also refused to summon and examine (certain) witnesses, thus demonstrating its prejudicial attitude towards the applicant companies. The applicant companies also disputed the lower court’s conclusion that the publicly available information had been sufficient for the Commission to reach its decision. They considered that, in reality, the Commission had not added any piece of unclassified evidence to the case file to support its presumptions that the applicant companies posed a threat to national security. The applicant companies also considered that the adding of non-public documents (*nevieši dokumentai*) to the file had been in breach of their procedural guarantees. If the State institutions wished to rely on such documents, the SSD firstly had to declassify them.

58. The applicant companies asseverated that they had no intention of connecting the data storage facility to the FSB’s Radio-Electronic Intelligence Centre in the Russian Federation. The Commission’s assumption in this regard had been far-fetched and technologically unfeasible. The applicant companies could not understand what threat their project posed to national security.

59. Lastly, they argued that the protocol decision breached their right to protection of property.

60. The Commission and the SSD, who had been a third party in the proceedings, asked the Supreme Administrative Court to dismiss the applicant companies’ appeal.

61. By a ruling of 30 May 2018, the Supreme Administrative Court noted that the Commission’s protocol decision no. NS-49 of 24 November 2017 (see paragraphs 37-39 above) “was based, among other things, on classified documents” (*įslaptinti dokumentai*) provided by the SSD to the Commission, and that those documents formed the factual basis for the protocol decision. The Supreme Administrative Court noted that “[to date] the classified material [had] not been included in the case file [before it], and [that it was] necessary in order to assess whether the Commission’s protocol decision was lawful and reasoned”. The Supreme Administrative Court thus ordered the SSD to provide those documents to it (see also paragraph 29 above).

62. Afterwards, having examined the case in written proceedings, by a ruling of 27 June 2018, the Supreme Administrative Court dismissed the appeal by the two applicant companies and SatGate Holding ApS and left the lower court’s decision unchanged.

63. The Supreme Administrative Court found that the Commission's protocol decision did comply with the requirements set out in Article 8 § 1 of the Law on Public Administration (see paragraph 72 below), since it was based on specific legislative provisions which had been applied to specific facts. It further held that "it could be understood (*galima suvokti*) from the content of the Commission's decision the factual and legal basis" on which the decision was based, from which it followed that the applicant companies' right to a defence in court (*teisė į teisminę gynybą*) had not been curtailed.

64. Neither Arcus Novus nor SatGate Holding ApS had contested the fact that they both fell under the status of potential participants within the meaning of Article 2 § 2 of the Law on Enterprises and Facilities of Strategic Importance; accordingly, the Commission had had reason to assess their compliance with the interests of national security. Under Article 7 § 10 (4) of that Law, a potential participant was acknowledged as complying with the interests of national security provided that it had no links to foreign States' special services.

65. The Supreme Administrative Court then stated that its panel had "examined the evidence as presented in the case file and reached the conclusion that the publicly available factual evidence provided by the SSD confirm[ed] that the companies SatGate Holding ApS and Arcus Novus [had] links to the FSB of the Russian Federation". Taking into account all the circumstances relevant to the case, and on the basis of the criteria of fairness and reasonableness, there was no basis for rejecting or declaring unsubstantiated the public information (*vieši duomenys*) that had been provided to the Commission by the SSD on which the Commission's findings had been based.

66. The Supreme Administrative Court also observed that the first-instance court had thoroughly and comprehensively examined the information forming the basis of the Commission's decision; therefore, essentially sharing the conclusions of the first-instance court, it held that it would not in detail assess the matters set out in the appeal relating to the assessment of the public information provided by the SSD.

67. The Supreme Administrative Court noted that in reaching its decision, "the first-instance court had also relied on classified information provided by the SSD". In that context, the Supreme Administrative Court referred to Article 56 § 3 of the Law on Administrative Proceedings, which provided that, as a rule, information which was a State or official secret could not be used as evidence in administrative proceedings unless it had been declassified (see paragraph 73 below). Nevertheless, that provision did not impose an absolute ban on the use of information constituting a State or official secret as evidence in an administrative case. When using non-declassified information as evidence it was important to take into account that "no court decision" could be based exclusively on information constituting a State secret (or other classified information) which was not known to the parties

(or one party) to the case. On this point, the Supreme Administrative Court referred to the Constitutional Court’s ruling of 15 May 2007 (see paragraph 75 below).

68. Notwithstanding this issue, and even if “the first-instance court [had] reasonably agreed that the classified information was allowed as evidence in the applicant companies’ case”, this had not breached their procedural rights, given that the non-classified evidence in the case file allowed for “a reasonable conclusion” that Arcus Novus and SatGate Holding ApS had links to the secret services of foreign States, this criteria having been referred to in Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance (see paragraph 70 below). Likewise, the first-instance court, having admitted classified information in evidence in the administrative case and assessed that with other (non-classified) evidence in the case file in accordance with the rules for the assessment of evidence set out in Article 56 § 6 of the Law on Administrative Proceedings, had not departed from the practice of the Supreme Administrative Court, the Constitutional Court and the Court regarding the interpretation of how classified information could be used as evidence.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

69. The Constitution reads:

Article 30

“A person whose constitutional rights or freedoms are violated shall have the right to apply to a court. ...”

Article 46

“Lithuania’s economy shall be based on the right of private ownership, freedom of individual economic activity and initiative.

The State shall support economic efforts and initiative that are useful to society.

The State shall regulate economic activity so that it serves the general welfare of the Nation. ...”

70. The relevant provisions of the Law on Enterprises and Facilities of Strategic Importance to National Security and Other Enterprises of Importance to Ensuring National Security (*Strateginė reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas*) at the material time read as follows:

Article 2: Definitions

“1. National security interests mean protection of the independence and sovereignty of the State, European and transatlantic integration, reducing threats and risks to energy and other economic sectors of fundamental importance to public security.

2. Potential participant means a natural or legal person that has officially declared an intention or interest in investing in an enterprise of strategic or considerable importance to national security, or in investing in an enterprise established or operating in an economic sector of considerable strategic importance to national security, or acquiring ownership, management or any other rights to facilities of particular strategic or strategic importance to national security. An existing shareholder of an enterprise of strategic or considerable importance to national security seeking to acquire additional shares in the enterprise shall also be considered a potential participant.

...

4. Enterprises and facilities of strategic or considerable importance to national security and facilities of particular strategic or strategic importance to national security means enterprises located or being established and facilities being designed or constructed in the Republic of Lithuania which, according to their purpose and/or nature of activities, are, under this Law, assigned particular strategic, strategic or considerable importance to national security and which, due to the protection of essential interests of national security, are subject to conditions and requirements regarding ownership, management or any other rights to the enterprises or facilities, the capital structure of the enterprises and changes therein, as well as requirements to be complied with by potential participants.”

Article 3: State and municipal enterprises of strategic importance to national security and facilities belonging to the State by right of ownership

“3. The following economic sectors shall be of considerable strategic importance to national security:

...

3) information technology and telecommunications, and other high technology;

...”

Article 7: Assessment of compliance of potential participants with national security interests

“1. Assessment of compliance of potential participants with national security interests shall be carried out in the manner and cases stipulated herein.

2. Assessment of compliance of a potential participant with national security interests shall be carried out in the cases where [he, she, it]:

...

2) acting independently or, in the cases specified by the Law on Securities, jointly with other persons acting together, seeks to acquire the shares which, together with the shares already held by [him, her, it] or together with the shares held by other persons acting together, grant over 1/3 of the votes in an enterprise of strategic or considerable importance or an enterprise operating in the economic sector of considerable strategic importance to national security indicated in Article 3(3) of this Law;

...

10. A potential participant shall be recognised as complying with national security interests provided that [he, she or it]:

1) meets the criteria of European and transatlantic integration ...;

...

3) does not maintain relations with institutions of foreign States which are not members of the European Union and the North Atlantic Treaty Organisation or with persons from those States which might increase the risk or pose a threat to national security;

4) there is no information that a person has relations with ... the special services ... of foreign States...;

...

11. If the Commission finds that a potential participant does not comply with national security interests, the decision must indicate the legal and factual basis. A negative decision by the Commission means that the State objects to that person becoming a potential participant and that person may not become a potential participant in the manner referred to in paragraph 2 until [he, she or it] eliminates the reasons for [his, her or its] non-compliance with national security interests and the Commission has taken a new decision confirming compliance of that person with national security interests.

12. The decision of the Commission may be appealed against before the Vilnius Regional Administrative Court in accordance with the procedure established by the Law on Administrative Proceedings of the Republic of Lithuania.”

71. The Law on Investments (*Investicijų įstatymas*) at the material time read as follows:

Article 8: Areas of investment

“1. Investment in the Republic of Lithuania shall be permitted in all lawful commercial and economic activities, subject to the restrictions established by this Law and other laws of the Republic of Lithuania.

2. Foreign investment shall be prohibited in commercial and economic activities guaranteeing State security and defence (except for investment by foreign entities meeting the criteria of European and transatlantic integration which Lithuania has opted for, provided this is approved by the State Defence Council).

3. Investment in an economic sector of strategic importance for ensuring national security ... shall only be permitted after having assessed the compliance of the investor with national security interests and in accordance with the cases and procedure established by [the Law on Enterprises and Facilities of Strategic Importance].”

72. The Law on Public Administration (*Viešojo administravimo įstatymas*) at the material time read:

Article 8: General requirements for an individual administrative decision and notification of the adoption of an individual administrative decision

“1. An individual administrative decision shall be based on objective information (facts) and provisions of law, and the sanctions applied (withdrawal of a licence or authorisation, temporary prohibition to engage in a particular activity or to provide services, imposition of a fine) shall be reasoned.”

73. The Law on Administrative Proceedings (*Administracinių bylų teisenos įstatymas*) at the material time read:

Article 56: Evidence

“1. Evidence in an administrative case is all factual information found admissible by the court hearing the case and based on which the court finds ... that there are circumstances which justify the claims and rebuttals of the parties to the proceedings, and other circumstances which are relevant to the fair disposal of the case, or that there are no such circumstances ...

3. As a rule (paprastai), factual information which constitutes a State or official secret may not be used as evidence in an administrative case, until the information has been declassified in a manner prescribed by law.

...

6. No evidence before the court shall have a predetermined effect. The court shall assess the evidence according to its inner conviction based on a detailed, comprehensive and objective review of all the circumstances of the case on the basis of the law, as well as the criteria of justice and reasonableness.”

74. In its ruling of 6 May 1997, the Constitutional Court held:

“As a rule, discrimination is understood as a change in the situation of a person or group of persons in relation to others without any objective justification. However, in certain cases, providing there exists a sufficiently reasoned and grounded cause, it is possible by law to establish a legal status for different groups of subjects and to consolidate certain particularities of the legal situation. That is to say, the constitutional principle of equality of persons does not negate the possibility of treating people differently according to their status.”

75. In its ruling of 15 May 2007, the Constitutional Court pointed out that no court decision could be based exclusively on information constituting a State secret (or other classified information) which was not known to the parties (or one party) to the case. The Constitutional Court held:

“11.

...

Taking account the fact that, on the one hand, the need to protect information constituting a State secret (or other classified information) is in the public interest, and, on the other hand, that the right of a person to a judicial remedy must be guaranteed, the law must establish under what grounds, procedure and conditions information constituting a State secret (or other classified information) can be accessed during the proceedings, provided the court decides that the information in question may be regarded as evidence in the case, as well as legal regulation of the relevant procedural actions in such a way as to ensure compliance with the constitutional principle of proportionality, to maintain a balance between the two above-mentioned constitutional values – the protection of State secrets (or other classified information) as a public interest, and the rights and freedoms of the individual, which are defended by that individual in court. There must be such legal regulation that the court may administer justice without denying any of these values.

Thus, the law must establish such legal regulation that, on the one hand, a party to the proceedings may request certain information which constitutes a State secret (or other classified information) to be admitted as evidence in the relevant case (if such information, in the opinion of that party, has evidentiary value) and, on the other hand,

the court must decide each time whether such a request is justified and whether it may be granted (in full or in part) by law, whether if it is granted (in full or in part) the public interest (to ensure the protection of State secrets (or other classified information)), as well as the values entrenched in the Constitution, and defended and protected by it, *inter alia*, the rights and freedoms of others, and the international obligations of the Republic of Lithuania, will not be harmed. The above-mentioned right of the party to a case to request that information which constitutes a State secret (or other classified information) be recognised as evidence in the relevant case in itself does not imply that the court must grant such a request (in full or in part), or that the party must have access to the information constituting a State secret (or other classified information); whether certain information constituting a State secret (or other classified information) may be evidence in a case depends on a number of factors which must be taken into account by the court. In this context, it should be mentioned that, as held by the Constitutional Court, the public interest is dynamic and subject to change (the Constitutional Court's rulings of 8 July 2005 and 21 September 2006); it is very diverse, therefore, it is virtually impossible to say *a priori* in which areas of life, where legal disputes may arise or in which it may be necessary to apply the law (*inter alia*, to protect secrets which must be protected in accordance with the international obligations of the Republic of Lithuania), the public interest may be threatened, or it may be necessary to ensure the public interest by means of interference by public institutions or their officials. Thus, it is impossible to define (list) *a priori* all situations where information which constitutes a State secret (or other classified information) cannot be recognised as evidence by a court decision, and therefore the parties to the case may not access such information. However, it is clear that if evidence (material) which does not constitute a State secret (or other classified information) is sufficient for the court to adopt a decision in the case and to administer justice as entrenched in the Constitution, this information not subject to disclosure should not, in order to protect the public interest, be evidence in that case and the parties to the case may not access it.

It should be emphasised that the court considering a case has a special responsibility when deciding whether certain information constituting a State secret (or other classified information) may be recognised as evidence in the case.

...

12. At the same time, it should be emphasised that no court decision can be exclusively based on information constituting a State secret (or other classified information) which is unknown to the parties (or one party) to the case."

76. In its ruling of 24 January 2014, the Constitutional Court held:

"6.2. It should be noted that the fundamental constitutional values established in Article 1 of the Constitution – the independence of the State, democracy and the republic – are closely related to the geopolitical orientation of the State of Lithuania established in the Constitution, which presupposes the European and transatlantic integration chosen by the Republic of Lithuania. As the Constitutional Court noted in its ruling of 7 July 2011, the geopolitical orientation of the State of Lithuania means membership of the Republic of Lithuania in the EU and NATO and the need to fulfil the relevant international obligations related to that membership. It should also be noted that such geopolitical orientation of the State of Lithuania is based on the recognised and protected universal constitutional values which are common with the values of other European and North American States."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 6 § 1 OF THE CONVENTION

77. The applicant companies complained that they had not had a fair hearing when challenging the Commission’s decisions finding that they did not comply with the interests of national security in the administrative courts. They submitted that the administrative courts had refused them access to decisive evidence, which had been classified and thus withheld from them. In that context, the applicant companies also alleged that they had been denied certifications owing to the Lithuanian authorities’ anti-Russian sentiment.

In support of their complaints, the applicant companies relied on Articles 6, 13 and 14 of the Convention.

78. The Court, being the master of characterisation to be given in law to the facts of the case (see, *Radomilja and Others v. Croatia* [GC], nos. 37685/10 and 22768/12, § 126, 20 March 2018), considers that the applicant companies’ complaints fall to be examined under Article 6 § 1 of the Convention, the relevant part of which reads as follows:

“In the determination of his civil rights and obligations ... everyone is entitled to a fair ... hearing ... by [a] ... tribunal ...”

A. Admissibility

1. *The parties’ submissions*

(a) **The Government**

79. The Government did not contest the fact that the present case concerned a “dispute” between the applicant companies, as potential participants in a sector of strategic importance, and the Commission. The main subject of the dispute had been the assessment of the applicant companies’ compliance with national security interests, and the legal consequences arising as a result of the unfavourable decisions adopted in that regard. The Commission’s decisions had therefore had an effect on the applicant companies’ civil rights. In fact, domestic law, namely Article 7 § 12 of the Law on Enterprises and Facilities of Strategic Importance, provided that a natural or legal person with an interest could appeal against the Commission’s decisions (see paragraph 70 above). The applicant companies had availed themselves of that opportunity.

80. Having regard to the above, the Government agreed that Article 6 § 1 of the Convention, under its civil limb, was applicable to the administrative proceedings at issue.

81. They submitted, however, that the applicant companies’ complaint of a lack of a fair hearing and adversarial proceedings was manifestly ill-founded.

(b) The applicant companies

82. The applicant companies shared the Government's position that the present case concerned a "dispute" between them and the Commission, over the latter's decisions hindering their development of the data centre project. The Commission's decisions had thus clearly had an effect on their civil rights. They submitted that Article 6 § 1 of the Convention, under its civil head, was applicable to the administrative court proceedings at issue.

83. The applicant companies disagreed that their complaint was unfounded.

2. The Court's assessment

84. The Court firstly notes that the dispute between the applicant companies and the Commission examined by the administrative courts concerned the assessment of the applicant companies' compliance with national security interests in connection with their intention to develop and build a data centre and the companies' merger (see paragraphs 5, 7, 10, 11, 37-39 above). It therefore considers that their grievances related to the fairness of those court proceedings fall to be examined under the civil head of Article 6 § 1 of the Convention. The applicability of that provision to the circumstances of the present case and the applicant companies' complaint not having been contested by the Government (see paragraph 79 above), the Court sees no reason to hold otherwise.

85. The Court further notes that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicant companies

86. The applicant companies argued that, at the time of adoption of the Commission's decisions, they had not been provided with any information or documents confirming the conclusions reached in those decisions, on the basis of which their freedom of economic activity had been restricted.

87. They further considered that if the Lithuanian courts found that particular material constituted a State or official secret, they were obliged to turn to the originator (source) of such information, with a request for its declassification. It was the applicant companies' understanding that, in their case, the Lithuanian authorities had been required to firstly declassify this information in order to subsequently rely on it in a dispute between the parties. However, as regards the Commission's first protocol decision, issued on 16 August 2016, the classified documents had been relied on by the Supreme Administrative Court, without the applicant companies having had

access to that information. In that manner, the applicant companies had been denied the right to be informed of the grounds and allegations that they posed a threat to national security, those proceedings having ended by the Supreme Administrative Court's ruling of 27 June 2018.

88. The situation had been similar regarding the possibility of effectively contesting the Commission's second protocol decision, issued on 24 November 2017.

89. The applicant companies further considered that, in both sets of administrative proceedings, every decision of the Commission and the courts had been based solely on the classified documents never disclosed to them. Although they had asked the courts not to accept such documents as evidence, the courts had decided otherwise. As a result, they had been prevented from effectively defending their rights in court against unreasonable and unlawful decisions based entirely on classified information.

90. The applicant companies also disagreed that publicly available information, as well as unclassified information added to the case file by the SSD and the Commission, sufficed for the Commission to reach its findings that they failed to meet the requirements of Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance. In their view, the Commission had not adduced any evidence in support of its allegations concerning the applicant companies being a threat to Lithuania's national security. The applicant companies had not been apprised of any preliminary information on which the Commission's findings as to their threat to national security had been based. Yet, branding the applicant companies a threat to national security had damaged their reputation beyond repair. In their application form lodged in November 2018, they had also stated that, "for the past couple of years, due to political events, the general background [could] be regarded as anti-Russian", which included the SSD publishing recommendations against Russian companies and Russian business, and that "all decisions against Russian companies [were] perceived with a connotation that an anti-Lithuanian threat [had been] discovered and disbanded".

91. On the facts, the applicant companies asseverated that although some of their shareholders were indeed Russian nationals, this did not mean they posed a threat to national security. They did not deny that V.A. had previously worked for a subsidiary of Gazprom; however, that was public information listed on V.A.'s LinkedIn profile; they had never hidden it. Quoting the applicant companies, it was "ridiculous" to think that individuals who were Russian spies would list the single fact revealing them as such (employment history) on their LinkedIn profile. Conversely, no other facts proving that V.A. was or had been working for the FSB or companies linked to the FSB had been presented and disclosed either by the Commission or by the SSD. Similarly, the mere fact that V.A. was a Russian citizen should not be considered as proof that in Lithuania he was a threat to national security. The applicant companies thus argued that, for the Lithuanian authorities, "being

Russian” was tantamount to “being a Russian spy”. Holding such a view was discriminatory and disproportionate. Given the above, it could be concluded that publicly available information could not constitute a sufficient basis for a decision that the applicant companies posed a threat to national security. Rather, it confirmed that decision had been based solely on classified information not disclosed to them.

92. The applicant companies did not deny that all the parties to the proceedings, including themselves, had provided unclassified and publicly available information to the administrative courts at different stages of the proceedings. However, they disagreed with the Government’s position that the publicly available information substantiated and confirmed the lawfulness or reasonableness of the unfavourable decisions taken in respect of them by the Commission and, subsequently, the administrative courts.

93. Contrary to what had been suggested by the Government (see paragraph 105 below), the mere fact that the applicant companies had made various procedural requests and taken an active role in the proceedings did not change the fact that their right to a fair hearing had been infringed, for those actions and requests had yielded no results.

94. In sum, the applicant companies submitted that they had not had a fair hearing when challenging the Commission’s decisions in the administrative courts, those courts having relied on classified documents provided by the SSD. The applicant companies could not, however, contest the accusations against them, pursuant to which they had been declared “enemies of the State”, whereas the decisions of the Commission were claimed to be a victory of the SSD in the mass media, calling it a victory stopping unfriendly Russian activities in Lithuania, and ensuring security in cyberspace. This was in clear breach of the principle of equality of arms, and in violation of Article 6 § 1 of the Convention.

(b) The Government

95. At the outset, the Government submitted that the applicant companies operated in the information technology and telecommunications sector, which was considered to be of strategic importance for ensuring national security. The framework for screening investors and assessing their compliance with national security interests had been prompted by the need to safeguard the national security interests of the Republic of Lithuania, also in the light of its geopolitical orientation (the Government referred to, among other, the Constitutional Court’s ruling of 24 January 2014, see paragraph 76 above), and freedom of economic activity was not absolute. Besides, such screening was normal practice within the European Union.

96. The right to adversarial proceedings was a fundamental principle of Lithuanian law, as pointed out by the Supreme Administrative Court in its practice, that court also having noted the importance of that principle when questions of acceptance of classified documents as evidence in administrative

proceedings arose. According to the consistent case-law of the administrative courts, a court judgment based solely on classified material could not be recognised as reasonable and lawful. Similarly, whilst the Constitutional Court had also held that, “as a rule”, classified information could not be relied on as evidence in administrative case, it had nevertheless pointed out that exceptions to that rule were possible, where a need to protect the public interest arose (see paragraph 75 above).

97. In the applicant companies’ case, the first-instance court had asked the SSD to declassify the classified information submitted in the administrative case; however, the SSD had refused to do so because the term for the declassification of classified information had not yet expired and the need for classification remained. As regards the appellate proceedings, after the Supreme Administrative Court had obtained access to the classified documents, it had found no reason to doubt the reasonableness of their classification; otherwise, that court would, of its own initiative, have raised the question of declassification of the material, as such an opportunity had been clearly formulated in the well-established case-law of the Supreme Administrative Court.

98. In this regard, the Government pointed out that after notice had been given of the present case, they had applied to the SSD asking it to declassify the classified documents examined by the courts in the two sets of administrative proceedings. On 9 November 2020 the SSD had replied that the need for classification remained, as declassification of this information could harm the activities of the SSD, and that therefore the classified documents could not be declassified.

99. That notwithstanding, the Commission’s protocol decisions had contained detailed elements that had led to the adoption of the unfavourable decisions in respect of the applicant companies.

100. During the oral hearings which had taken place before the Vilnius Regional Administrative Court, it should have been clear to the applicant companies and their lawyers from the questions posed to the witnesses V.A. and V.M. that it was the relations or connections of the shareholders of the applicant companies (and/or the companies related to them) with the Russian security and intelligence services which posed a threat to the national security of Lithuania. The content of the oral hearings had demonstrated even more clearly the specific circumstances which had been relevant to the proceedings at issue and which the applicant companies or their witnesses had had to comment on or provide explanations about. As the applicant companies had been able to comprehend what specific relations and under which circumstances they were considered to pose a threat to national security, they had been able to defend themselves against those allegations against them.

101. As regards specific documents provided to the parties and the courts at each stage of the court proceedings, the Government noted that all the parties to the proceedings, including the applicant companies, had provided

unclassified and publicly available information to the administrative courts at different stages of the proceedings (see paragraphs 16 and 41 above).

102. The classified information provided by the SSD during the administrative proceedings had not been of decisive value; it had supplemented a large amount of publicly available information, which had been available to both the parties to the proceedings (including the applicant companies) and courts at two levels. Both publicly available and classified information had substantiated and confirmed the lawfulness and reasonableness of the unfavourable decisions taken in respect of the applicant companies by the Commission and, subsequently, the courts.

103. Further, compliance of a potential participant (investor) from the point of view of national security was assessed on an individual basis, based on factual information. As could be seen from the statistics provided by the Commission, since 2016 it had recognised a total of twenty-eight potential participants (investors) (natural or legal persons) as not complying with national security interests, nine of which had been Russian citizens. In other cases, potential investors had been from Lithuania, Latvia, Estonia, Italy and other European Union countries. Thus, the statistical data provided by the Commission demonstrated that it was not the nationality of the potential participant (investor) that determined the assessment of the potential participant's (investor's) compliance with national security interests.

104. The applicant companies had not been discriminated against on the basis of the nationality of their shareholders, such as V.A. When assessing the compliance of potential participants (investors) in economic sectors of strategic importance for ensuring national security, the SSD normally paid greater attention to the following: (i) potential participants (investors) from third countries (especially from Russia, Belarus and China); (ii) potential participants (investors) who had carried out or were carrying out activities in those countries; and (iii) potential participants (investors) who had or had had relations (commercial, personal and so forth) with individuals from those countries. It should be explained that particular attention was given to the above-mentioned potential participants (investors) due to the activities of the intelligence and security services of Russia, Belarus and China, and the policy pursued by these countries towards the Republic of Lithuania. However, in any case, the mere fact that the potential participant (investor) was related to nationals of the above-mentioned States did not in itself constitute grounds for alleging that the potential participant (investor) posed a threat to national security.

105. Last but not least, as could be seen from a number of procedural requests by the applicant companies that had been granted by the administrative courts, the applicant companies had been able to effectively exercise their procedural rights and guarantees. No obstacles to the defence had been created, and the administrative courts had followed all the necessary procedures to avoid any unnecessary restrictions. Any limitation had been

sufficiently counterbalanced by the procedures followed by independent and impartial judicial authorities which had played an active role in the proceedings and had thus provided not only adequate safeguards to protect the interests of the applicant companies but had also struck a fair balance between the State's interests and those of the applicant companies.

106. In the light of the above, the Government concluded that in the case at issue the right to a fair hearing and, in particular, the principles of adversarial proceedings and equality of arms, for the purposes of Article 6 § 1 of the Convention, had not been infringed.

2. *The Court's assessment*

(a) **General principles**

107. The Court's case-law regarding the principle of adversarial proceedings and the principle of equality of arms, which are closely linked, and are fundamental components of the concept of a "fair hearing" within the meaning of Article 6 § 1 of the Convention, are summarised in *Regner v. the Czech Republic* ([GC], no. 35289/11, §§ 146-49, 19 September 2017):

"146. The Court reiterates that the adversarial principle and the principle of equality of arms, which are closely linked, are fundamental components of the concept of a "fair hearing" within the meaning of Article 6 § 1 of the Convention. They require a "fair balance" between the parties: each party must be afforded a reasonable opportunity to present his case under conditions that do not place him at a substantial disadvantage *vis-à-vis* his opponent or opponents (see *Avotiņš v. Latvia* [GC], no. 17502/07, § 119 and other references, ECHR 2016).

147. However, the rights deriving from these principles are not absolute. The Court has already ruled, in a number of judgments, on the particular case in which precedence is given to superior national interests when denying a party fully adversarial proceedings (see *Miryana Petrova [v. Bulgaria]*, no. 57148/08, §§ 39-40[, 21 July 2016] and *Ternovskis [v. Latvia]*, no. 33637/02, §§ 65-68[, 29 April 2014]). The Contracting States enjoy a certain margin of appreciation in this area. However, it is for the Court to determine in the last instance whether the requirements of the Convention have been complied with (see, for example, *Tinnelly & Sons Ltd and Others and McElduff and Others v. the United Kingdom*, 10 July 1998, § 72, *Reports of Judgments and Decisions* 1998-IV; *Prince Hans-Adam II of Liechtenstein v. Germany* [GC], no. 42527/98, § 44, ECHR 2001-VIII; and *Devenney v. the United Kingdom*, no. 24265/94, § 23, 19 March 2002).

148. The Court reiterates, moreover, that the entitlement to disclosure of relevant evidence is not an absolute right either. In criminal cases it has found that there may be competing interests, such as national security or the need to protect witnesses at risk of reprisals or keep secret police methods of investigation of crime, which must be weighed against the rights of the party to the proceedings. However, only measures restricting the rights of a party to the proceedings which do not affect the very essence of those rights are permissible under Article 6 § 1. For that to be the case, any difficulties caused to the applicant party by a limitation of his or her rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities (see, *mutatis mutandis*, *Fitt v. the United Kingdom* [GC], no. 29777/96, § 45 with other references,

ECHR 2000-II, and *Schatschaschwili v. Germany* [GC], no. 9154/10, § 107, ECHR 2015).

149. In cases where evidence has been withheld from the applicant party on public interest grounds, the Court must scrutinise the decision-making procedure to ensure that, as far as possible, it complied with the requirements to provide adversarial proceedings and equality of arms and incorporated adequate safeguards to protect the interests of the person concerned (see *Fitt*, cited above, § 46)."

(b) Application of the general principles to the present case

108. The Court observes that, in accordance with the requirements of Lithuanian law, during the legal proceedings concerning the lawfulness and reasonableness of the Commission's protocol decisions assessing the applicant companies' compliance with national security interests, those companies faced two restrictions: firstly, the classified documents and information on which the Commission had based its findings were not made available either to the applicant companies or to their lawyers, and secondly, those classified documents were not disclosed to the applicant companies during the proceedings in the administrative courts, who referred to that classified information when upholding the Commission's findings. The Court accordingly has the task of examining whether those restrictions infringed the very essence of the applicant companies' right to a fair hearing (see, *mutatis mutandis*, *Regner*, cited above, § 150).

109. In carrying out that examination, the Court will have regard to the proceedings considered as a whole and will determine whether the restrictions on the adversarial and equality-of-arms principles, as applicable in the civil proceedings, were sufficiently counterbalanced by other procedural safeguards (see *Regner*, cited above, § 151).

110. On the facts of the case, the Court observes that when reaching its protocol decision no. NS-23, the Commission referred to the SSD's report no. 19-1379, which set out and explained the reasons for considering the second applicant company a threat to national security (see paragraph 10 above). The Commission's second protocol decision no. NS-49 contained a similar assessment regarding the second applicant company's risk to Lithuania's national security, and also referred to the facts stated in the Commission's first decision (see paragraph 38 above). As explained by the Government (see paragraph 97 above), the classified information that had been provided by the SSD to the Commission, was not disclosed to the applicant companies.

111. That being so, the Court observes that the Commission's first protocol decision rather explicitly described the reasons behind the Commission's findings. Namely, it referred to elements such as the specific names of Arcus Novus and its related companies' shareholders, including V.A., who, because of his links to the Gazprom-related companies, was considered a threat to Lithuania's national security. As noted by the

Supreme Administrative Court, the applicant companies essentially did not contest the circumstances related to V.A.'s employment history (see paragraph 51 *in fine* above). The Commission's protocol decision likewise provided an assessment of why a data centre project, such as that envisioned by the applicant companies, would be a risk to Lithuania's national security (see paragraph 10 above). Besides the aforementioned information, the Commission's second protocol decision also referred to the fact that even if V.A. were to sell his shares in Arcus Novus, he would still retain influence in that company (see paragraph 38 *in fine* above). Regarding the fairness of the proceedings before the Commission, the Court also observes that, given that the information which the applicant companies initially provided to the Commission was not comprehensive or entirely disclosed, the latter gave those companies an opportunity to supplement it with information concerning some of its specific shareholders (see paragraph 36 above). That being so, the Court finds that already at the stage of the Commissions' decisions, copies of which were provided to the applicant companies (see paragraphs 12, 42 and 46 above), those companies should have at least been aware of the basis for the Commission's decisions not to give clearance for the intended business operation. This conclusion is supported by the Supreme Administrative Court's finding that "it [could] be understood from the content of the Commission's decision the factual and legal basis" on which it was based, from which it followed that the applicant companies' right to a defence had not been curtailed (see paragraph 63 above).

112. The Court next turns to the proceedings in the administrative courts in which the applicant companies challenged the Commission's decisions.

113. The Court firstly finds that the amount of information available to the parties, including the applicant companies, increased throughout the court proceedings, which essentially concerned the same issue. According to the information in the Court's possession, the Commission, the Chancellery and the SSD provided numerous pieces of unclassified material including: both protocol decisions of the Commission, documents regarding the applicant companies' shareholder structure, copies of replies from the Lithuanian law-enforcement authorities, the presentation of the data centre project, and the SSD's six-page long response to the applicant companies' appeal (see paragraphs 15, 17, 43 and 44 above). This being the case, it is therefore reasonable to hold that the applicant companies and their lawyers were kept apprised of the relevant evidence, as far as was possible without the material which the SSD sought to keep secret on public interest grounds being disclosed to them (see paragraphs 21 and 98 above), and insofar were permitted to make submissions and participate in the decision-making process during the administrative proceedings. The Supreme Administrative Court, having examined all the material in the case file and the classified material, concluded in its decision of 27 June 2018 that it was clear from the publicly available factual evidence provided by the SSD that the applicant

companies did not satisfy the statutory conditions set forth in Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance (see paragraphs 64 and 65 above).

114. Secondly, the Court finds that the applicant companies have actively participated in the administrative court proceedings to effectively defend their interests. During the proceedings before the first-instance court, oral hearings were held, and the information gathered was examined directly, in the presence of the applicant companies' representatives and their lawyers (see paragraphs 23 and 45 above). The Court also finds it paramount that, at the applicant companies' own request, one of the principal actors, V.A., who had been criticised for his links to Gazprom-related companies (see paragraphs 10 and 38 above), as well as V.M., were examined during both sets of court proceedings (see paragraphs 22 and 45 above). The lack of any kind of predisposition against the applicant companies by the administrative courts is further supported by the fact that numerous other requests by them were granted: the courts agreed to adjourn hearings when the applicant companies could not participate or when they wished to conclude a settlement with the Commission (see paragraph 22 above) or to expedite the court proceedings in view of their grievance that they would incur losses if the proceedings were protracted (see paragraph 27 above). That being so, the Court finds that the decision-making during the administrative court proceedings ensured that, as far as possible, the applicant companies and their lawyers were given an opportunity to effectively participate, without jeopardising the confidentiality of evidence which it was necessary to withhold in the public interest, an issue which the Court will examine next.

115. Regarding the applicant companies' grievance that classified evidence was relied on to support the finding that they could not qualify as potential participants within the meaning of Article 2 § 2 of the Law on Enterprises and Facilities of Strategic Importance, the Court cannot agree with their claim that the administrative courts disregarded their right to adversarial proceedings and right to equality of arms on account that the classified information was not disclosed to them. Firstly, the Court points out that the Vilnius Regional Administrative Court inquired with the producer of that information, the SSD, whether the classified information could be declassified, and that its answer was negative as the need to keep the information classified remained (see paragraph 21 above). In these circumstances, whilst it is true that the classified information was disclosed to the Commission and later to the administrative courts (see paragraphs 10, 14, 19, 29, 30, 55 and 61 above), the Court notes, in particular, that the material which was not disclosed in the present case to the applicant companies formed only a certain part of the overall evidence on which the Commission's protocol decisions and the courts' findings were based (see paragraphs 30, 51, 65 and 68 above). In particular, and in line with the Supreme Administrative Court's practice, based on Article 56 § 6 of the Law

on Administrative Proceedings (see paragraphs 68 and 73 above), as well as in line with the position of the Constitutional Court (see paragraph 75 above), the classified information does not appear to have been of decisive value in the proceedings (see also paragraph 102 above). It was corroborated by numerous unclassified documents, such as the information submitted to the domestic courts by the Commission, the Chancellery and the SSD (see paragraphs 15, 17, 18, 43 and 44 above), the State authorities' responses regarding the applicant companies (see paragraphs 7, 35 and 43 above), as well as information submitted by the companies themselves, including when the initial information submitted to the Commission had been contradictory and not fully disclosed (see paragraphs 8 and 36 above). In such circumstances, the Court concludes that the circumstances of the instant case differ from those examined by the Court in *Pocius v. Lithuania* (no. 35601/04, 6 July 2010), in which an "operational records file" was deemed to be essential evidence of the applicant's alleged danger to society and, having examined it behind closed doors, the Lithuanian judges merely presented their conclusions to him. As concluded by the Supreme Administrative Court in the instant case, even if "the first-instance court [had] reasonably agreed that the classified information was allowed as evidence in the applicant companies' case", this had not breached their procedural rights, given that the unclassified evidence in the case file allowed for a reasonable conclusion that, because of their connections with the secret services of foreign States, the applicant companies failed to meet the criteria set forth in Article 7 § 10 (4) of the Law on Enterprises and Facilities of Strategic Importance (see paragraph 68 above).

116. The Court also takes notice of the Government's arguments regarding Lithuania's geopolitical orientation, entrenched both in the domestic statutory law and in the Constitutional Court's jurisprudence (see Article 2 § 1 in paragraph 70 above, Article 8 § 2 in paragraph 71 above, and the Constitutional Court's ruling in paragraph 76 above). As the instant case is related to the applicant companies' economic activity (see paragraphs 6 and 7 above), the Court also takes notice of the domestic courts' findings that the matter was related to issues of national security, and that, according to the case-law of the Supreme Administrative Court, the rights of the individual could not supersede those of the nation and national security (see paragraph 50 above). The Court has already held that it is not for it to take the place of the States Parties to the Convention in defining their national interests, a sphere which traditionally forms part of the inner core of State sovereignty (see, *mutatis mutandis*, *Stoll v. Switzerland* [GC], no. 69698/01, § 137, ECHR 2007-V, and *Zarubin and Others v. Lithuania* (dec.), no. 69111/17, § 54, 26 November 2019). Besides, the Court has held that the right to disclosure of all relevant evidence is not absolute and may be subject to restrictions designed to protect the rights of third parties or an important public interest such as national security (see, *mutatis mutandis*, *Regner*, cited

above, § 148). There is nothing in the case at issue to suggest that the classification of the documents in question was carried out arbitrarily. Any arbitrariness on the part of the Commission was also ruled out by the administrative courts, which held that it had reached reasonable decisions and followed the letter of the law (see paragraphs 33, 55 *in fine*, 56 and 63 above).

117. Having regard to the proceedings as a whole, to the nature of the dispute and to the margin of appreciation enjoyed by the national authorities, the Court finds that the domestic law and practice of the administrative courts in the case at issue provided the required level of protection to the applicant companies. The courts duly exercised the powers of scrutiny available to them and the special responsibility required from them in this type of proceedings (see paragraph 68 above; see also the Constitutional Court's ruling in paragraph 75 above), both regarding the need to preserve the confidentiality of classified documents and regarding the assessment of the reasonableness and lawfulness of the Commission's protocol decisions, giving reasons for the courts' decisions with regard to the specific circumstances of the present case (see *Regner*, cited above, § 154). The Court thus considers that the restrictions curtailing the applicant companies' enjoyment of the rights afforded to them in accordance with the principles of adversarial proceedings and equality of arms were offset in such a manner that the fair balance between the parties was not affected to such an extent as to impair the very essence of the applicant companies' right to a fair hearing.

118. Consequently, there has been no violation of Article 6 § 1 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 1 OF PROTOCOL No. 1 TO THE CONVENTION

119. The applicant companies further complained that the decisions of the Commission and the administrative courts barring them from successfully developing and finishing the data centre project amounted to a breach of their right to protection of property, as guaranteed by Article 1 of Protocol No. 1 to the Convention, which reads as follows:

“Every natural and legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.”

A. The parties' submissions

1. The Government

120. The Government firstly argued that the applicant companies could not have had any legitimate expectations with regard to the development of the data storage facility. The applicable provisions of domestic law had been sufficiently accessible, precise and foreseeable in their application, and the applicant companies should have been aware that they would be subject to the screening procedure established under Article 7 of the Law on Enterprises and Facilities of Strategic Importance, as also noted in Article 8 § 3 of the Law on Investments (see paragraph 71 above). The applicant companies should have taken this fact into account prior to engaging in any developments of the data storage facility project.

121. The aforementioned legislation governing issues related to the assessment of investors' compliance with national security did not give legal entities unlimited rights to participate in activities of economic sectors important for ensuring national security. The Government reiterated that the applicant companies operated in the information technology and telecommunications sector, which was considered to be an economic sector of strategic importance for ensuring national security. Such sectors, taking into account their specifics and nature, needed higher standards of protection from, among other things, external impact from countries "which [were] unfavourable to the State of Lithuania in terms of their geopolitical orientation or natural and legal persons closely linked to their policies". Besides, under the doctrine of the Constitutional Court, freedom of economic activity was not absolute. In the case of the applicant companies, the Supreme Administrative Court also referred to the need to protect the information technology and telecommunications sector from possible external impact from countries unfavourable to Lithuania (see paragraphs 64 and 65 above). In that context, the Government also referred to the settled case-law of the Supreme Administrative Court to the effect that when either under the legal regulation or by other acts, the State or State institutions did not undertake any obligations in respect of the persons concerned, no legitimate expectations arose for the applicants. In other words, when the applicants only had a mere hope, which had no legal basis in domestic law, their complaints were dismissed by the administrative courts as unfounded. In its case-law, the Supreme Administrative Court had emphasised that legitimate expectations could only be based on the provisions of legislation in force.

122. The Government also stated that the applicant companies had failed to exhaust domestic remedies given that they had not brought proceedings against the State for damages. Such proceedings had been available and capable of dealing with the essence of the complaint and providing redress as concerns the alleged violation of Article 1 of Protocol No. 1 to the Convention, namely any financial losses allegedly incurred due to the

Lithuanian authorities' decisions preventing the data storage facility. Yet, no such allegations had been addressed by the domestic courts.

2. *The applicant companies*

123. The applicant companies objected to the Government's position that they had had no legitimate expectations with regard to the development of the data storage facility. They submitted that they had been developing the data centre project and had invested substantial amounts of money in it. Yet, after the decisions of the Commission and the courts, it had been impossible to successfully conclude the project: they had been left unable to acquire the necessary licences and permits, they had lost their investors and contractors, and there remained no prospect of contracting clients while being branded a threat to national security. The investments they had already made had been lost.

124. The applicant companies had had legitimate expectations of developing the data centre project without what they considered to be groundless interference by the State authorities. Likewise, they had had a legitimate expectation that the Commission would not find them a threat to national security only because some of their shareholders were Russian nationals. Similarly, the applicant companies could not have predicted that V.A.'s prior work experience in Gazprom-related companies might be an issue when going through the investment screening procedure.

125. The applicant companies also noted that, regarding the lawfulness of the Commission's decisions, they had lodged claims with the administrative courts. A claim for damages, however, could not be seen as an effective domestic remedy: such a claim had not offered any reasonable prospect of success in terms of remedying the unlawfulness of the Commission's decisions barring the applicant companies from developing the data centre project. Under domestic law, unlawful actions were a condition *sine qua non* when awarding damages. Accordingly, a claim for compensation would have been ineffective, since the Lithuanian courts had not annulled the decisions that the applicant companies were a threat to national security.

126. Lastly, the applicant companies had not been obliged to exhaust every possible remedy: having appealed against the decisions of the Commission, they had not been required to seek compensation, which had had the same objective and had not provided any chance of success, even theoretically. Besides, they had raised, at least in substance, all the main arguments, including those related to losses incurred due to their having been prevented from developing the data centre project, which were subsequently raised before the Court, thus giving the domestic courts an opportunity to address them.

B. The Court's assessment

127. The Court finds that it does not have to address the Government's objection that the applicant companies should have lodged a claim for damages, such a claim also having been mentioned by the domestic court (see paragraph 24 *in fine* above), since the complaint is in any event inadmissible for the reasons described below.

128. The relevant principles as to when a claim may be regarded as an "asset" and therefore a "possession" enjoying protection under Article 1 of Protocol No. 1 are summarised in its judgment in the case of *Radomilja and Others* (cited above, §§ 142-43 and 149) and the cases cited therein. A claim may be so regarded when it has a sufficient basis in national law or, in other words, when it is sufficiently established as to be enforceable (*ibid.*, § 142). In the absence of such a claim, an applicant cannot argue that he or she has a "legitimate expectation" that it will be realised, that is, that he or she will obtain effective enjoyment of a property right (see *Kopecký v. Slovakia* [GC], no. 44912/98, §§ 48-49, ECHR 2004-IX).

129. Furthermore, since it is in the first place for the national authorities, notably the courts, to interpret and apply domestic law, the Court will not call into question the way in which domestic courts have done so unless their interpretation and application of domestic law is arbitrary or manifestly unreasonable (see *Radomilja and Others*, cited above, § 149). Likewise, it is not the Court's task to substitute its own assessment of the facts for that of the domestic courts because, as a general rule, it is for those courts to assess the evidence before them. Although the Court is not bound by the findings of domestic courts, in normal circumstances it requires cogent elements to lead it to depart from the findings of fact reached by those courts (*ibid.*, § 150). It is for these reasons that, in principle, it cannot be said that an applicant has a sufficiently established claim amounting to an "asset" for the purposes of Article 1 of Protocol No. 1 where there is a dispute as to the correct interpretation and application of domestic law and where the question whether he or she complied with the statutory requirements is to be determined in judicial proceedings (*ibid.*, § 149).

130. The Court notes the Government's argument that, under Lithuanian law, a potential participant in an economic sector of strategic importance must undergo a screening procedure so that its compliance with the interests of national security are assessed (see paragraph 70 above). This was the situation in the present case, and, as noted by the domestic court, Arcus Novus and SatGate Holding ApS did not deny that those rules and requirements had applied to them (see paragraph 64 above; see also, *mutatis mutandis*, *Hutten-Czapska v. Poland* [GC], no. 35014/97, § 163 *in fine*, ECHR 2006-VIII). Given that as a result of that screening the Commission concluded that the applicant companies did not meet the required criteria, and that the reasonableness and lawfulness of the Commission's protocol decisions were

confirmed by the administrative courts, whose decisions contain no cogent elements that would lead the Court to find them arbitrary or manifestly unreasonable, it must be concluded that the applicant companies, who were represented by lawyers throughout the proceedings, could not have had a legitimate expectation that they would be allowed to successfully develop and finish the data centre. No legitimate expectation can be said to arise where there is a dispute as to the correct interpretation and application of domestic law and the applicant's submissions are subsequently rejected by the national courts (see *Kopecký*, cited above, § 50).

131. It follows that this part of the applicant companies' complaint is inadmissible as being incompatible *ratione materiae* with the provisions of the Convention or the Protocols thereto within the meaning of Article 35 § 3 (a) and that it must be rejected pursuant to Article 35 § 4.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the complaint under Article 6 § 1 of the Convention concerning the fairness of the proceedings regarding the Commission's protocol decisions admissible and the remainder of the application inadmissible;
2. *Holds* that there has been no violation of Article 6 § 1 of the Convention.

Done in English, and notified in writing on 13 June 2023, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Dorothee von Arnim
Deputy Registrar

Arnfinn Bårdsen
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Derenčinović is annexed to this judgment.

A.R.B.
D.V.A.

CONCURRING OPINION OF JUDGE DERENČINOVIĆ

1. I agree with the decision that, in this case, the authorities did not violate the applicant companies' rights under Article 6 of the Convention. Given that this is a borderline case, the main reason for my position is the fact that the national authorities justified the interference with the applicant companies' fair trial rights on the grounds of national security. It is a well-established practice of the Court that in the domain of national security, States have a very wide margin of appreciation when it comes to derogable rights.

2. Nevertheless, regardless of the support on the merits, I am afraid I must disagree with some parts of the reasoning which, in my opinion, depart from the standards and principles established in the recent practice of the Court. Specifically, I believe that in such a sensitive borderline case, which encroaches on the very foundations of the right to a fair trial, it was necessary to carry out a detailed analysis of the counterbalancing factors put in place by the national authorities and to determine whether they meet the high standards of this Court. Detailed analysis and close scrutiny of those factors (compensatory measures) are necessary in order to strike the requisite balance between the security interests of the State and the individual's right to a fair trial. Unfortunately, this in-depth analysis is missing.

3. Another shortcoming in the reasoning concerns the reference to the findings of the national courts about the "geopolitical orientation" of the State. I find very problematic the fact that the reasoning seems to endorse this contextual argument, as it has no support either in the text of the Convention or in the case-law of the Court.

4. In the following paragraphs I will briefly address these two shortcomings.

5. The reasoning in the context of the general assessment, including in terms of counterbalancing factors, relies heavily on *Regner v. the Czech Republic* ([GC], no. 35289/11, 19 September 2017). The reference to that judgment is not the most appropriate for several reasons. First, certain controversial findings in *Regner* were the subject of some justified and well-reasoned criticism in separate opinions, and the judgment was not adopted with a clear consensus among the members of the composition. Thus, for example, Judge Sajó correctly concluded in his dissenting opinion that the majority's position that "the adversarial principle and the principle of equality of arms are not absolute" did not derive from the Court's previous case-law (see *Regner*, cited above, dissenting opinion of Judge Sajó, § 11). To support this position, the majority relied on *Fitt v. the United Kingdom* ([GC], no. 29777/96, ECHR 2000-II) and *Schatschaschwili v. Germany* ([GC], no. 9154/10, ECHR 2015). However, as correctly pointed out by Judge Sajó, the Court did not address the absolute (or relative) nature of the right to equality of arms and adversarial proceedings in those two cases. It simply reiterated that the right to access a court was not absolute, which is not the

same as the equality-of-arms issue. In addition, Judge Sajó was correct in pointing out that the judgments referred to by the majority in *Regner* “... are inapposite because neither contemplates an applicant being completely denied access to evidence: in both *Fitt* and *Schatschaschwili* the applicants were prevented from cross-examining witnesses, but they were provided with fully transcribed copies of witness testimony. This is not so in the present case, where none of the incriminating evidence, not even a summary of the *substance* of the charges, was communicated to the applicant” (see *Regner*, cited above, dissenting opinion of Judge Sajó, § 12). This logic can also be applied, *mutatis mutandis*, to the present case, because the classified information which the competent State authorities refused to declassify was in no way, even indirectly, available to the applicant companies. For this reason, reference to certain findings from *Regner*, which departs from the Court’s previous case-law, appears not to be justified.

6. Furthermore, the reasoning in the present judgment seems to overlook the important standards on counterbalancing factors established recently in *Muhammad and Muhammad v. Romania* ([GC], no. 80982/12, 15 October 2020). That judgment is *lex posterior* in relation to *Regner* and is perhaps a more appropriate precedent for the present case given that it dealt with general national security concerns in relation to foreign nationals, while *Regner* dealt with a purely domestic issue of security clearance in the context of employment. Although in *Muhammad and Muhammad* (cited above) the Court found a violation of Article 1 of Protocol 7 and not of Article 6 of the Convention, its analysis was heavily influenced by fair trial (due process) considerations and was carried out in a manner characteristic of the assessment of the fair trial guarantees. The *Muhammad and Muhammad* standards further specify the conditions under which counterbalancing factors can be considered proportionate in the context of restrictions on individual rights for national security reasons. These standards are relevant because they confirm that a system in which procedural rights are only formally guaranteed, and in which effective participation in the proceedings by a person whose rights were restricted due to national security reasons is not ensured, does not meet the requirements established under the Convention. Put simply, such proceedings lack the basic due process guarantees.

7. In other words, the *Muhammad and Muhammad* standards specify that effective participation in the proceedings implies, *inter alia*, the awareness or knowledge of the person whose right is being restricted as to the factual elements on the basis of which the national authorities considered that person to represent a security threat. Given that the applicant companies, in this case, did not have access to the evidence based on classified data, it is not entirely clear from the reasoning whether they could have been aware of the circumstances based on facts from publicly available sources which – although it is unclear to what extent – were also part of the case file. This

question is crucial for assessing whether the applicant companies' effective participation in the proceedings was ensured.

8. What can be concluded from the reasoning of this judgment is that some of the applicant companies' requests were accepted, such as the one for adjournment of the hearing and speeding-up of the proceedings (see paragraph 114 of the judgment), but what is missing is an analysis of the extent to which their meritorious requests necessary for the final resolution of the case were indeed considered by the authorities. Without such an analysis it is difficult to determine whether the applicant companies' effective, and not just formal, participation in the proceedings was ensured. I firmly believe that applying the standards established in *Muhammad and Muhammad* would avoid this shortcoming in a borderline case like this and make the reasoning more convincing.

9. The first part of paragraph 116 of the judgment reads as follows:

“The Court also takes notice of the Government's arguments regarding Lithuania's geopolitical orientation, entrenched both in the domestic statutory law and in the Constitutional Court's jurisprudence (see Article 2 § 1 in paragraph 70 above, Article 8 § 2 in paragraph 71 above, and the Constitutional Court's ruling in paragraph 76 above). As the instant case is related to the applicant companies' economic activity (see paragraphs 6 and 7 above), the Court also takes notice of the domestic courts' findings that the matter was related to issues of national security, and that, according to the case-law of the Supreme Administrative Court, the rights of the individual could not supersede those of the nation and national security (see paragraph 50 above).”

10. It sounds very odd for a human rights court to endorse in such a general manner, even in the form of taking notice, the collective interests of the State over the rights of individuals guaranteed under the Convention. A reference to “geopolitical orientation”, a term that cannot be found either in the Convention or in its interpretation by the Court, seems inappropriate even in the form of taking notice, despite the fact it might be enshrined in the constitutional and statutory framework of a particular State Party. Taking fully into account the context of the case, I am thoroughly convinced that such an unusual discourse should have been reconsidered, particularly in a delicate borderline case such as this.